EUROOPAN UNIONIN TIETOSUOJAUUDISTUS

- ERITYISESTI REKISTERINPITÄJÄN NÄKÖKULMASTA

Lapin yliopisto

Oikeustieteiden tiedekunta

Oikeusinformatiikka

Petteri Rinkinen

Maisteritutkielma

Kevät 2014

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Euroopan unionin tietosuojauudistus – erityisesti rekisterinpitäjän näkökulmasta
Tekijä: Rinkinen Petteri
Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka
Työn laji: Maisteritutkielma
Sivumäärä: XII + 87 sivua
Vuosi: 2014

Tiivistelmä:

Perustuslain 10.1 §:ssä määrätään, että henkilötietojen suojasta tulee säätää lain tasoisella säädöksellä. Tämä merkitsee, että henkilötietojen suoja on perusoikeustasoinen oikeus. Nykyisin henkilötietojen suojasta on säädetty henkilötietolaissa (523/1999), joka perustuu henkilötietodirektiiviin (95/46/EY).

Euroopan unionin tasolla on vireillä lainsäädäntöhanke, jonka tarkoituksena on saattaa voimaan kokonaisvaltainen uudistus koskien henkilötietojen suojaa. Tavoitteena on, että vastaisuudessa henkilötietojen suojasta säädettäisiin asetuksella (COM(2012) 11 final). Tämä edesauttaisi yhtenäisen henkilötietojen suojan tason saavuttamisessa unionin tasolla. Tällä hetkellä henkilötietojen suojasta säädetään kansallisissa säädöksissä, jotka eroavat huomattavasti toisistaan.

Tässä tutkimuksessa on keskitytty erityisesti siihen mitä uusi henkilötietojen suojaa sääntelevä asetus merkitsee voimaantullessaan rekisterinpitäjille. Näkökantana on ollut erityisesti se millaisia velvoitteita ja vastuita uusi asetus mahdollisesti tuo rekisterinpitäjille ja henkilötietojen käsittelijöille sekä se miten nämä velvoitteet eroavat nykyisin voimassa olevista säännöksistä. Erityisesti vertailua on suoritettu henkilötietolakiin, mutta soveltuvilta osin näkökantaan on otettu vertailuun myös erityislainsäädäntö. Vertailuun on otettu mukaan myös asetusehdotusta käsitteleviä lausuntoja siltä osin kun niissä on käsitelty rekisterinpitäjiä koskevia asetusehdotuksen artikloita.

Avainsanat: henkilötietojen suoja, henkilötietolaki, henkilötietodirektiivi, Euroopan unionin tietosuojauudistus

SISÄLLYS

LÄHTEET

Kirjallisuus:

Aarnio, Reijo. Ohjelmistoteollisuudelle mahdollisuus. Tietosuoja -lehti 3/2012. Stellatum Oy.

Alapuranen, Leena. Henkilötietojen käsittelyn yleiset lähtökohdat. Teoksessa: Henkilötietojen käsittely työelämässä. Muut kirjoittajat: Koskinen Seppo, Lehtonen Lasse ja Heino Anna-Maija. Edita Publishing Oy 2012.

Bygrave, Lee A. Data Protection Law Approaching Its Rationale, Logic and Limits. Kluwer Law International. The Hague, London, New York 2002.

Civilka, Mindaugas ja Barasneviciute, Rita. Data protection and privacy: Changing interplay with human rights. Teoksessa: Saarenpää Ahti (toim.) Legal privacy. Zaragoza : Prensas Universitarias de Zaragoza 2008.

Eklund, Mia C. ja Lilja, Johanna. Kuluttajien profilointi markkinointitarkoituksiin – Henkilötietojen käsittelyn ja tietosuojasääntelyn kehityssuuntia. Defensor Legis 2/2013. Suomen asianajajaliitto.

Järvinen, Petteri. Tietoturva & yksityisyys. Docendo Oy. Jyväskylä 2002.

Koillinen, Mikael. Henkilötietojen suoja itsenäisenä perusoikeutena. Oikeus 2/2013. Oikeuspoliittinen yhdistys Demla ry ja Oikeus- ja yhteiskuntatieteellinen yhdistys ry.

Korhonen, Rauno. Perusrekisterit ja tietosuoja. Edita Prima Oy. Helsinki 2003.

Korhonen, Rauno. Sähköinen asiointi ja viestintä. Teoksessa: Tammilehto Timo (toim.) Oikeusjärjestys 2012, osa 3. Lapin yliopisto. Rovaniemi.

Lagus, Antti J. Varaudu uhkiin järjestelmällisesti. Tietosuoja -lehti 1/2013. Stellatum Oy.

Magnusson Sjöberg, Cecilia. E-samhället. Teoksessa: Rättsinformatik Inblickar i e-samhället, e-handel och e-förvaltning. Muut kirjoittajat: Nordbeck Peter, Norden Anna ja Westman Daniel. Studentlitteratur AB 2012.

Makkonen, Kaarle. Luentoja yleisestä oikeustieteestä. Helsingin yliopisto 1998.

Männikkö, Päivi. Tietosuojavaltuutetun toimisto 25 vuotta. Tietosuoja -lehti 4/2012. Stellatum Oy.

Männikkö, Päivi. Uusi tietosuojalainsäädäntö: Yhteisille säännöille kyllä, byrokratialle ei. Tietosuoja -lehti 4/2012. Stellatum Oy.

Neuvonen, Riku. Viestintä- ja informaatio-oikeuden perusteet. Lakimiesliiton kustannus 2013.

Neuvonen, Riku. Viestintäoikeuden perusteet. Talentum. Helsinki 2008.

Nyyssölä, Mikko. Yksityisyyden suoja työsuhteessa. WS Bookwell Oy 2009.

Ollila, Riitta. Henkilötietojen vapaa liikkuvuus ja viestintä. Teoksessa: Viestintäoikeus. Muut kirjoittajat: Kulla Heikki, Koillinen Mikael, Kuopus Jorma, Lavapuro Juha, Lehtonen Lasse, Nieminen Hannu, Pohjolainen Teuvo, Pöysti Tuomas, Sorvari Hannu, Sorvari Katariina, Tähti Aarre, Viljanen Veli-Pekka ja Wallin Anna-Riitta. WSOY Lakitieto 2002.

Raatikainen, Ari. Yksityisyyden suoja työelämässä. Edita Oy. Helsinki 2002.

Saarenpää, Ahti. Henkilö- ja persoonallisuusoikeus. Teoksessa: Tammilehto Timo (toim.) Oikeusjärjestys 2012, osa 1. Lapin yliopisto. Rovaniemi.

Saarenpää, Ahti. Finland. Teoksessa: Blume Peter (toim.) Nordic data protection. Kauppakaari. Helsinki 2001.

Salminen, Markus. Tietosuoja sähköisessä liiketoiminnassa. Talentum 2009.

Schartum, Dag Wiese. Norway. Teoksessa: Blume Peter (toim.) Nordic data protection. Kauppakaari. Helsinki 2001.

Seipel, Peter. Sweden. Teoksessa: Blume Peter (toim.) Nordic data protection. Kauppakaari. Helsinki 2001.

Syrjänen, Pentti. Yksityisyyden suoja ja henkilöarviointi. Akateeminen väitöskirja. Tampereen Yliopistopaino Oy 2006.

Tiilikka Päivi. Teoksessa Henkilötietojen suoja. Muut kirjoittajat: Pitkänen Olli ja Warma Eija. Talentum Helsinki 2013.

Vanto, Jarno J: Henkilötietolaki käytännössä. WSOYpro Oy. Helsinki 2011.

Voutilainen, Tomi. ICT-oikeus sähköisessä hallinnossa - ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Edita Publishing Oy. Helsinki 2009.

Öman, Sören ja Lindblom, Hans-Olof. Personuppgiftslagen En kommentar. Norstedts Juridik AB. Stockholm 2001.

Virallislähteet:

Ehdotus: Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), COM(2012) 11 final, annettu: Bryssel 25.1.2012.

Ehdotus: Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta, COM(2012) 10 final, annettu: Bryssel 25.1.2012.

Euroopan parlamentti: Euroopan parlamentin lainsäädäntöpäätöslauselma 12. maaliskuuta 2014 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely)

Euroopan parlamentin Oikeudellisten asioiden valiokunta (JURI): Lausunto oikeudellisten asioiden valiokunnalta kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen

käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), annettu 25. maaliskuuta 2013.

Datainspektionen. Ruotsin tietosuojaviranomaisen www-sivut.
Osoitteessa: http://www.datainspektionen.se/

Datatilsynet. Norjan tietosuojaviranomaisen www-sivut.
Osoitteessa: http://www.datatilsynet.no/

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

Muttilainen, Vesa. Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistilastojen tietoja 1990-luvulta ja 2000-luvun alusta. Oikeuspoliittisen tutkimuslaitoksen julkaisuja. Helsinki 2006.

Regeringskansliet. Personal Data Protection. Information on the Personal Data Act.
Osoitteessa: http://www.regeringen.se/content/1/c6/07/43/63/0ea2c0eb.pdf

The Swedish data inspection board. Guidelines for companies. Responsibility for personal data processed in whistleblowing systems.
Osoitteessa: http://www.datainspektionen.se/Documents/vagledning-whistleblowing-eng.pdf

The Swedish data inspection board. What on earth the data inspection board do?
Osoitteessa:http://www.datainspektionen.se/Documents/datainspektionen-presentation-eng.pdf

Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä, 20. kesäkuuta 2007.
Osoitteessa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fi.pdf

Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista (00530/12/FI WP 191), annettu 23. maaliskuuta 2012.

Tietosuojatyöryhmän lausunto. Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, annettu 30. toukokuuta 2002.
Osoitteessa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf

Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus.
Osoitteessa: http://www.tietosuoja.fi/uploads/068sox3cia0ww.pdf
Päivitetty 27.07.2010

Tietosuojavaltuutetun toimisto. Rekisterinpitäjä.
Osoitteessa: http://www.tietosuoja.fi/27232.htm

Tietosuojavaltuutetun toimisto. Tietoa rekisterinpitäjälle.
Osoitteessa: http://www.tietosuoja.fi/1698.htm

Tietosuojavaltuutetun toimisto. Tietosuojan ja tietoturvan ”tee se itse”-tarkastus.
Osoitteessa: http://www.tietosuoja.fi/uploads/qmdum.pdf Päivitetty 27.07.2010

Tietosuojavaltuutetun toimisto. Tietosuojatyöryhmä.
Osoitteessa: http://www.tietosuoja.fi/14891.htm

Tietosuojavaltuutetun toimisto. Tietosuojavastaavan toimenkuva, tehtävät ja asema.
Osoitteessa: http://www.tietosuoja.fi/uploads/939r21bdr3_1.pdf Päivitetty 27.07.2010

Tietosuojavaltuutetun toimisto. Toimialakohtaisten käytännesääntöjen laatiminen. Osoitteessa: http://www.tietosuoja.fi/uploads/xcia0786nsyg.pdf Päivitetty 27.07.2010

Tietosuojavaltuutetun toimisto. Yhdysvaltalainen Safe Harbor-järjestelmä. Osoitteessa: http://www.tietosuoja.fi/25914.htm

Viestintävirasto. Ohje tietoturvallisuuden arviointilaitoksille. Osoitteessa: https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf (annettu 7.5.2013)

Viestintävirasto. Tietoturvaloukkausilmoitus. Osoitteessa: https://www.viestintavirasto.fi/tietoturva/teleyritystenoikeudetjavelvollisuudet/tietoturvaloukkausilmoitus.html (päivitetty 9.2.2013)

Viestintävirasto. Tietoturvallisuuden arviointilaitokset. Osoitteessa: http://www.viestintavirasto.fi/tietoturva/tietoturvallisuudenarviointilaitokset.html

Internet-osoitteet:

Väkeväinen Heidi: Palveluntarjoajan velvollisuus ilmoittaa tietoturvaloukkauksesta täsmentyy. Merilampi Oy. Osoitteessa: http://www.merilampi.com/uutiskirjeartikkelit?artikkeli=33810480

Muut lähteet:

Euroopan parlamentin lehdistötiedote. Mepit äänestivät vahvemman henkilötietojen suojan puolesta. Osoitteessa:http://www.europarl.europa.eu/pdfs/news/expert/infopress/20140307IPR38204/20140307IPR38204_fi.pdf (annettu 12.3.2014)

Euroopan unionin komission lehdistötiedote. Progress on EU data protection reform now irreversible following European Parliament vote.

Osoitteessa: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

Euroopan unionin komission lehdistötiedote. Tietosuoja: komissio tukee Yhdysvaltojen kanssa tehtävää "safe harbor" –sopimusta.

Osoitteessa: http://europa.eu/rapid/press-release_IP-00-301_fi.htm

Korhonen, Rauno. Diat: Informaatiohallinnon päivä 2012.

LYHENTEET

ETA	**Euroopan talousalue**
EU	**Euroopan unioni**
HE	**Hallituksen esitys**
HetiL	**Henkilötietolaki (523/1999)**
IP-osoite	**Internet protocol address, internet protokollan osoite**
ISO 27001	**Tietoturvastandardi**
JURI	**Euroopan parlamentin Oikeudellisten asioiden valiokunta**
LIBE	**Civil Liberties, Justice and Home Affairs, Kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta**
OECD	**Organisation for Economic Cooperation and Development, Taloudellisen yhteistyön ja kehityksen järjestö**
Pk-yritykset	**Pienet ja keskisuuret yritykset**
PL	**Suomen perustuslaki (731/1999)**
PuL	**Personuppgiftslagen (1998:204)**

1 JOHDANTO, TUTKIMUKSEN ESITTELY JA KESKEISET KÄSITTEET

1.1 Johdanto

Tässä maisteritutkielmassa käsitellään Euroopan unionin henkilötietojen suojaa koskevan lainsäädännön uudistushanketta. Uudistushankkeen kokonaisuuteen kuuluu ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojeluksi henkilötietojen käsittelyssä sekä näiden tietojen vapaaksi liikkuvuudeksi (yleinen tietosuoja-asetus).[1] Nykyisin henkilötietojen suojasta säädetään direktiivin muodossa olevalla henkilötietodirektiivillä. Uudistushankkeen tavoitteena on, että jatkossa yleisestä henkilötietojen suojasta säädettäisiin asetuksella. Tutkielmassa on keskitytty käsittelemään yleisen tietosuoja-asetusehdotuksen neljättä lukua eli artikloita 22 - 39, jotka koskevat lähinnä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia. Uudistushankkeeseen kuuluu myös Euroopan parlamentin ja neuvoston direktiiviehdotus, joka koskee viranomaisten suorittamaa henkilötietojen käsittelyä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaata liikkuvuutta.[2]

Tutkielmassa käsiteltävä aihe on ajankohtainen, sillä tietosuojaan EU:n tasolla liittyy lukuisia ongelmia. Ensinnäkin erot siinä, miten kukin jäsenvaltio on implementoinut EU-lainsäädännön omaan kansalliseen lainsäädäntöönsä, ovat johtaneet henkilötietojen suojan eroihin eri jäsenvaltojen kesken. Toiseksi myös itse henkilötietoja koskeva lainsäädäntö on jäänyt jälkeen teknologian nopean kehittymisen takia. Kun henkilötietoja suojaavaa lainsäädäntöä on alun perin säädetty, moniakaan tämän päivän teknologian sovelluksia ei ole vielä ollut olemassa.[3]

Uusi teknologia on tarjonnut menetelmät käsitellä valtavia määriä tietoja nopeasti ja tehokkaasti. Yhteiskunnan kehityksen kannalta teknologisten innovaatioiden kehittäminen on luonnollisesti välttämätöntä. Toisaalta on syytä myös pitää mielessä, että uusi teknologia on tuonut mukanaan mahdollisuuden

[1] COM(2012) 11 final
[2] COM(2012) 10 final
[3] Korhonen. Dia nro 4. Informaatiohallinnon päivä 2012.

käyttää näitä uusia välineitä myös sellaisissa tarkoituksissa, joihin niitä ei suinkaan välttämättä alunperin ole kehitetty. Esimerkkinä voidaan mainita laaja yksilöiden seuraaminen ja valvonta, jonka nykyajan teknologia on olemassaololollaan mahdollistanut. Voitaneen perustellusti todeta, että jokaisella teknologisella innovaatiolla on yleensä toisaalta lukuisia hyviä puolia, mutta samalla se tuo mukanaan myös vähemmän hyviä mahdollisuuksia. Tässä kuvaan astuu yhteiskunnan velvollisuus asettaa tarkat rajat sille, mikä on sallittua ja minkä taas katsotaan loukkaavan oikeudettomasti yksilön oikeuksia.[4] Näitä rajalinjoja pyritään nimenomaan tietosuojan uudistuspaketissa määrittelemään entistä tarkemmin - erityisesti sitä silmällä pitäen, että yksilön oikeus yksityisyyteen ja muihin oikeuksiinsa pystyttäisiin juridisesti turvaamaan ja määrittelemään riittävän tehokkaasti.

Lähtökohtaisesti vertailua on tutkielmassa suoritettu nykyisin voimassa olevaan henkilötietodirektiiviin (95/46/EY) pohjautuvaan henkilötietolakiin (523/1999). Määrättyjen asioiden osalta vertailua on suoritettu soveltuvin osin myös tietosuojaa koskevaan erityislainsäädäntöön. Tutkielmassa on käsitelty myös tietosuojatyöryhmän virallista kannanottoa uudistushankkeeseen erityisesti niiltä kohdin, joissa on otettu kantaa rekisterinpitäjän velvoitteisiin.[5] Tämän lisäksi käsittelyyn on otettu myös Euroopan parlamentin oikeudellisten asioiden valiokunnan antama yleistä tietosuoja-asetusta koskeva lausunto – myös tämän lausunnon osalta näkökantana on tutkielmassa ollut rekisterinpitäjä.[6] Esittelyyn on otettu myös soveltuvilta osin Euroopan parlamentin maaliskuussa 2014 antama tietosuoja-asetusta koskeva lainsäädäntöpäätöslauselma.[7]

Henkilötietoasetusehdotuksen rakenne:

Luku I	Yleiset säännökset	
	1 artikla	Kohde ja tavoitteet
	2 artikla	Aineellinen soveltamisala

[4] Civilka ja Barasneviciute (2008), s. 208

[5] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista (00530/12/FI WP 191), annettu 23. maaliskuuta 2012.

[6] Lausunto oikeudellisten asioiden valiokunnalta kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), 25. maaliskuuta 2013.

[7] Euroopan parlamentti: Euroopan parlamentin lainsäädäntöpäätöslauselma 12. maaliskuuta 2014 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely)

	75 artikla	Oikeus oikeussuojakeinoihin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan
	76 artikla	Tuomioistuinmenettelyjä koskevat yhteiset säännöt
	77 artikla	Vastuu ja oikeus korvauksen saamiseen
	78 artikla	Seuraamukset
	79 artikla	Hallinnolliset seuraamukset
Luku IX	Tietojenkäsittelyyn liittyviä erityistilanteita koskevat säännökset	
	80 artikla	Henkilötietojen käsittely ja sananvapaus
	81 artikla	Terveyttä koskevien henkilötietojen käsittely
	82 artikla	Henkilötietojen käsittely työsuhteen yhteydessä
	83 artikla	Henkilötietojen käsittely historiantutkimusta taikka tilastollisia tai tieteellisiä tutkimustarkoituksia varten
	84 artikla	Salassapitovelvollisuus
	85 artikla	Kirkkojen ja uskonnollisten yhdistysten voimassa olevat tietosuojasäännöt
Luku X	Delegoidut säädökset ja täytäntöönpanosäädökset	
	86 artikla	Siirretyn säädösvallan käyttäminen
	87 artikla	Komiteamenettely
Luku XI	Loppusäännökset	
	88 artikla	Direktiivin 95/46/EY kumoaminen
	89 artikla	Suhde direktiiviin 2002/58/EY ja direktiivin muuttaminen
	90 artikla	Arviointi
	91 artikla	Voimaantulo ja soveltaminen

1.2 Tutkimuksen metodi, kohde ja rakenne

Oikeustiede voidaan nähdä toisaalta säännösten tulkintaan keskittyvänä lainoppina eli oikeusdogmatiikkana ja toisaalta se voidaan ymmärtää myös yleisluontoisena teoreettisempana suuntauksena, jossa keskeistä on itse oikeustieteen tieteellisen näkökulman tutkiminen ja edistäminen. Lainopissa selvitetään oikeuslähteistä saatavan tiedon avulla määrätyn oikeusyhteisön voimassa olevaa oikeutta.[8] Aina ei ole kuitenkaan mahdollista vetää tarkkaa rajaa lainopin ja yleisen oikeustieteen välille. Lukuisissa eri oikeudenaloilla esiin nousevissa lainopillisissa ongelmissa joudutaan turvautumaan yleisempään oikeustieteelliseen tutkimukseen, jotta lopputulos saadaan ratkaistuksi. Samaa ratkaisutapaa voidaan soveltaa myös päinvastoin. Tällöin yleisluonteiset

[8] Neuvonen (2013), s. 25

oikeudelliset ongelmat palautetaan yksittäistapauksiin, jolloin niiden ratkaiseminen luonnistuu määrätyissä tapauksissa helpommin.[9]

Tässä tutkielmassa metodistiseksi lähtökohdaksi on asetettu oikeusdogmaattinen näkökulma. Voimassa olevan lainsäädännön lisäksi tutkielmassa on toisaalta myös tulevaa lainsäädäntöä arvioiva näkökanta. Yleisenä kohteena tutkielmassa on tulevan tietosuoja-asetuksen arvioiminen ja sen selvittäminen miten se voimaan tullessaan eroaa nykyisin voimassa olevasta lainsäädännöstä.

Tutkielmassa erityiseksi näkökannaksi on valittu rekisterinpitäjään kohdistuva asetusehdotuksen sääntely. Tutkielmassa on pyritty erityisesti selvittämään millä tavoin tuleva tietosuoja-asetus vaikuttaa rekisterinpitäjän velvoitteisiin ja millä tavoin uudet määräykset eroavat nykyisin voimassa olevasta kansallisesta lainsäädännöstä. Vertailussa esille on nostettu myös lainsäädäntöhankkeesta annetut virallislausunnot ja erityisesti se, miten niissä esitetyt lainsäädäntöratkaisut eroavat rekisterinpitäjää erityisesti koskevien artikloiden osalta alkuperäisestä komission esityksestä.

Tutkielman alkuun on otettu keskeisimpiä käsitteitä määrittelevä jakso. Tämän jälkeen on käsitelty henkilötietojen suojan kansainvälistä ja kansallista kehitystä. Henkilötietolain yleistasoiselle esittelylle on varattu oma jakso. Tätä seuraa kansainvälinen osuus, jossa käsitellään lyhyesti Ruotsin, Norjan ja Yhdysvaltojen tietosuojaa koskevaa sääntelyä. Oikeusvertailulla pyritään yleensä selvittelemään eri oikeusjärjestysten suhdetta toisiinsa.[10] Tutkielman kansainvälisessä vertailussa kysymyksessä ei ole kuitenkaan varsinaisesti metodisessa mielessä oikeusvertailu vaan tarkoituksena on tuoda yleisesittelynä näkökulmaa siihen miten tietosuojaan liittyvät asiat on järjestetty esittelyyn otetuissa maissa. Kansainvälistä osiota seuraa tutkielmassa jaksot, joissa käsitellään unionin henkilötietojen suojaa koskevaa asetusehdotusta artikloittain samalla suorittaen vertailua Suomen nykyiseen lainsäädäntöön. Tämän jälkeen esittelyyn otetaan uudistusta käsittelevät virallislausunnot ja Euroopan parlamentin lainsäädäntöpäätöslauselma. Tutkielman lopussa

[9] Makkonen (1998), s. 3
[10] Makkonen (1998), s. 5

pohditaan miten lainsäädäntöhankeen jatko tästä etenee ja mitä muutoksia se voimaantullessaan mahdollisesti kansalliselle lainsäädännölle aiheuttaa.

1.3 Käsitteiden määritelmiä

Henkilötiedon käsite määritellään henkilötietolain 3 §:n ensimmäisessä momentissa: *Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.* Tällöin keskeistä on se, että tieto jonka avulla henkilö voidaan tunnistaa, on tallennettu alustalle. Sillä, mihin muotoon tieto on tallennettu, ei ole henkilötiedon käsitteen kannalta merkitystä. Tieto voi olla tällöin tallennettu esimerkiksi kirjalliseen tai sähköiseen muotoon. Sen sijaan pelkkää jotakin henkilöä käsittelevää puhetta ei pidetä henkilötietona, vaan sitä käsitellään esimerkiksi salassapitoa ja kunnianloukkausta koskevan lainsäädännön valossa.[11] Henkilötietoina voidaan tietosuojatyöryhmän mukaan pitää esimerkiksi IP-osoitteita, puhelunauhoitteita, röntgenkuvia sekä lääkemääräystietoja.[12]

Suomessa henkilötiedoilla tarkoitetaankin nimenomaan luonnollista henkilöä koskevia tietoja. Kaikkialla maailmassa henkilötiedon käsitettä ei ole rajattu koskemaan vain luonnollisia henkilöitä; esimerkiksi Itävallassa henkilötietojen suoja voi koskea myös yrityksiä.[13] On myös syytä muistaa, että aina ei ole helppo määritellä selkeästi onko määrätty yksittäinen tieto henkilötieto vai ei. Joissakin tilanteissa myös Suomessa yhteisöön viittaava tieto voi täyttää henkilötiedon määritelmän. Tällainen tilanne voi olla käsillä esimerkiksi silloin, kun tieto viittaa vain epäsuorasti yksilöön. Yksittäistä tapausta koskeva kokonaisvaltainen pohdinta ratkaisee lopulta onko tiedonjyvänen henkilötieto.[14]

Henkilötietojen käsittelyllä tarkoitetaan henkilötietolain mukaan *henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä*. Henkilötietolain luetteloa ei

[11] Alapuranen (2012), s. 41-42
[12] Tietosuojatyöryhmän lausunto 4/2007 henkilötietojen käsitteestä, 20. kesäkuuta 2007, www.ec.europa.eu/justice
[13] Vanto (2011), s. 22
[14] Bygrave (2002), s. 210

voida kuitenkaan pitää tyhjentävänä. Myös muut vastaavat toimet, jotka koskevat tavalla tai toisella henkilötietoja, voidaan katsoa tapauskohtaisesti henkilötietojen käsittelyksi. Henkilötietojen käsittelynä voidaan pitää lähtökohtaisesti kaikkia henkilötiedon elinkaaren aikana toteutettuja toimia henkilötietojen keräämisvaiheesta aina niiden tuhoamiseen asti.[15]

Henkilörekisterin käsite on määritelty henkilötietolain 3 §:ssä seuraavalla tavalla: *käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta*. Kuten sanamuodosta käy ilmi, niin henkilörekisteriksi ei katsota pelkästään sähköisessä muodossa olevia rekistereitä, vaan myös perinteisessä paperisessa muodossa olevat tietovarannot voivat muodostaa henkilörekisterin. Myös se, että tiedot hajotetaan toisistaan erillisiksi osiksi, esimerkiksi tietoteknisin keinoin, ei saa estää tietojoukon määrittelemistä henkilörekisteriksi. Keskeisenä seikkana määrittelyssä voidaan pitää tietojen yhteenkuuluvuutta.[16] Henkilörekisteri voidaan määritellä loogiseksi rekisteriksi. Tällöin keskeistä on, että henkilötiedot on kerätty tiettyä käyttötarkoitusta varten. Tällöin samaan loogiseen rekisteriin kuuluvat niin automaattisen tietojenkäsittelyn avulla ylläpidetyt rekisterinosat kuin myös manuaalisesti ylläpidetyt rekisterin osa-alueet.[17] Rekisteri, jossa on sekä luonnollisia henkilöitä että oikeushenkilöitä koskevia tietoja, on henkilörekisteri niiltä osin, joissa se sisältää luonnollista henkilöä koskevia henkilötietoja.[18]

Rekisterinpitäjällä tarkoitetaan henkilötietolain 3 § 4 kohdan mukaan *yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty*. On tärkeää henkilötietolain soveltamisen kannalta tietää kuka on milloinkin rekisterinpitäjä, jotta

[15] Alapuranen (2012), s. 45
[16] Saarenpää (2012), s. 319-320
[17] Tietosuojavaltuutetun toimisto. Tietoa rekisterinpitäjälle.
Osoitteessa: http://www.tietosuoja.fi/1698.htm
[18] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 3

rekisterinpitäjän velvoitteet voidaan kohdistaa oikean tahon toteutettavaksi.[19] Rekisterinpitäjän määritteleminen on myös siksi tärkeää, että henkilötietolakia sovelletaan lähtökohtaisesti vain silloin, kun rekisterinpitäjän toimipaikka on Suomessa tai Suomen oikeudenkäytön piirissä.[20] Keskeistä rekisterinpitäjän määrittelyssä on se, kuka käyttää rekisterinpidossa tosiasiallista määräysvaltaa. Tosiasiallisen määräysvallan merkkinä voidaan pitää esimerkiksi sitä kuka päättää siitä mitä tietoja kerätään ja miten tietoja kerätään.[21] Rekisterinpitäjäksi ei katsota tahoa, joka hoitaa vain rekisterin teknistä ylläpitoa.[22] Rekisterinpito on voitu myös määrätyissä tilanteissa lailla säätää jonkin tahon velvollisuudeksi. Yleensä tällaisessa lakimääräyksessä rekisterinpidon hoitamisesta huolehtiminen on säädetty jonkin viranomaisen tehtäväksi.[23]

Rekisteröidyn käsite määritellään lyhyesti henkilötietolain 3 §:n 5 kohdan mukaan henkilöksi, jota henkilötieto koskee. Henkilön tulee olla tunnistettavissa tiedosta, joka häntä koskee, jotta häntä voidaan pitää rekisteröitynä.[24] Tiedon tulee toisin sanoen olla yhdistettävissä joko suoraan tai välillisesti määrättyyn henkilöön. Suoraan tunnistettavana tietona voidaan luonnollisesti pitää henkilön nimeä sekä kuvaa. Välilliseksi tiedoksi voidaan puolestaan määritellä esimerkiksi henkilön asuinpaikkaan ja perheeseen liittyvät tiedot. Kun henkilö pystytään tunnistamaan näiden tietojen pohjalta, täyttyy rekisteröidyn käsitteen määritelmä. Käytännössä ongelmaksi nousee kuitenkin se, minkä tyyppistä tunnistettavuutta tällöin edellytetään. Toisin sanoen, täyttyykö rekisteröidyksi määritteleminen jo pelkästään silloin kun vain henkilön lähipiiri pystyy tunnistamaan hänet tiedoista vai vaaditaanko, että myös suurempi henkilön lähipiiriin kuulumaton joukko pystyy myös hänet tunnistamaan. Saarenpää näkee asian siten, että tällöin yksittäistapauksessa tilannetta on tulkittava sen henkilön oikeuksien eduksi jonka tiedoista on kysymys.[25]

Rekisteröidyn antama suostumus henkilötietojensa käsittelylle. Rekisteröidyn suostumus henkilötietojensa käsittelylle on periaate, joka kuuluu henkilötietojen

[19] Alapuranen (2012), s. 45
[20] Tietosuojavaltuutetun toimisto. Tietoa rekisterinpitäjälle.
Osoitteessa: http://www.tietosuoja.fi/1698.htm
[21] Tiilikka (2013), s. 56
[22] Alapuranen (2012), s. 46
[23] Tietosuojavaltuutetun toimisto. Rekisterinpitäjä.
Osoitteessa: http://www.tietosuoja.fi/27232.htm
[24] Alapuranen (2012), s. 48
[25] Saarenpää (2012), s. 333-334

käsittelyn yleisiin edellytyksiin henkilötietolain 8 §:n mukaisesti. Rekisteröidyn antama suostumus henkilötietojensa käsittelylle on ensisijainen peruste käsitellä yksilön henkilötietoja. Henkilötietolain 8 §:ssä käytetään ilmaisua *yksiselitteinen suostumus*. Suostumusilmauksen tulee olla tahdonilmaisuna selkeä ja sen tulee kohdistua tiettyä henkilötietojen käyttöä varten.[26] Suostumuksen tulee olla tietoinen, vapaaehtoinen ja yksilöity. Pätevä suostumus edellyttää rekisteröidyn riittävää tietoisuutta siitä minkälaista henkilötietojensa käsittelyä varten hän suostumuksensa antaa. Rekisterinpitäjällä on lisäksi epäselvyystilanteissa todistusvelvollisuus osoittaa suostumuksen olemassaolo.[27]

Sivullisena juridisessa mielessä pidetään henkilötietolain 3 §:n 6 kohdan mukaan *muuta henkilöä, yhteisöä, laitosta tai säätiötä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää tai henkilötietoja kahden viimeksi mainitun lukuun käsittelevää*. Sivullisen käsitteen erityisellä määrittelyllä - niin henkilötietodirektiivissä kuin tätä kautta myös henkilötietolaissa - on ilmeisesti haluttu painottaa erityisesti sitä kuka määritellään täysin ulkopuoliseksi suhteessa henkilötietojen käsittelyyn.[28]

2 TIETOSUOJALAINSÄÄDÄNNÖSTÄ

2.1 Tietosuojalainsäädännön kehityksestä

Yksityisyyden suojaamisella on pitkä historia. Esimerkiksi jo antiikin ajan Kreikassa Hippokrateen valassa lääkäri velvoitettiin pitämään salassa potilassuhteiden tiedot.[29] Juridisessa mielessä yksityisyyden historian juuret voidaan ajoittaa 1800-luvun lopun Yhdysvaltoihin. Kirjapainotekniikan yleistyminen oli lisännyt huomattavasti lehdistön levikkiä ja keskeiseksi kysymykseksi nousikin nopeasti missä kulkee yksityisen ja julkisen välinen raja. Juristipiireissä luotiin käsite ”oikeus olla yksin tai omassa rauhassa” (engl. the right to be let alone).[30]

[26] Saarenpää (2012), s. 351-353
[27] Salminen (2009), s. 55-56
[28] Tiilikka (2013), s. 60
[29] Salminen (2009), s. 19
[30] Korhonen (2003), s. 79-80

Kansainvälisessä mielessä henkilötietojen suoja nousi mielenkiinnon kohteeksi laajemmassa mittakaavassa 1960-luvulta alkaen. Keskeisenä syynä kiinnostukseen, joka heräsi henkilötietojen suojaamista kohtaan, oli tietotekniikan nopea kehittyminen. Uudella teknologialla pystyttiin keräämään ja käsittelemään tietoja sellaisella mittakaavalla, joka ei aiemmin ollut mahdollista.[31] Useissa maissa ilmestyi tutkimuksia ja selvitysraportteja yksityisyyden suojaamisesta. Muiden muassa Ruotsissa ilmestyi aiheesta kansallinen raportti vuonna 1972: *Data och integritet*. Ruotsi ottikin ensimmäisenä maana käyttöön yleisesti sovellettavan tietosuojalain jo vuonna 1973: *datalag*.[32] Myös Länsi-Saksassa alettiin osavaltiotasolla 1970-luvun alkupuolella säätää tietosuojaa koskevaa lainsäädäntöä. Tuon ajan tietosuojalainsäädäntöä kutsutaan yleisesti ensimmäisen sukupolven tietosuojalainsäädännöksi.[33]

Suomessa arvioitiin 1970-luvulla henkilötietojen suojaa koskevan lainsäädännön tarvetta, mutta varsinaiseen lainsäädäntöön asti poliittinen tahto ei vielä tuolloin riittänyt. Pitkällisen valmistelun tuloksena Suomeenkin saatiin oma henkilötietoja käsittelevä laki kun vuonna 1987 säädettiin henkilörekisterilaki (471/1987). Samassa yhteydessä säädettiin muutoksia myös muutamiin jo voimassa oleviin lakeihin. Henkilörekisterilaki tuli voimaan vuoden 1988 tammikuussa. Henkilörekisterilain voidaan katsoa olleen ns. toisen sukupolven tietosuojalaki. Henkilörekisterilaki oli luonteeltaan yleislaki, jota sovellettiin silloin, kun muussa laissa ei käsiteltävästä asiasta toisin säädetty.[34] Suomessa perinteisesti yksilön oikeuksia omiin henkilötietoihinsa oli aiemmin suojattu rikosoikeuden keinoin: esimerkiksi kotirauhaa ja intimiteettisuojaa koskevin säännöksin. Henkilörekisterilaki toi tähän ajattelutapaan merkittävän muutoksen sillä lain tavoitteena oli estää ennakolta mahdolliset henkilötietojen käsittelystä aiheutuvat yksityisyyden loukkaukset.[35]

Hyvän rekisteritavan noudattaminen näytteli keskeistä sijaa henkilörekisterilain soveltamisessa. Myös rekisterinpitäjien itsesääntelylle annettiin painava merkitys henkilörekisterilaissa. Henkilörekisterilaissa oli jo omaksuttu lukuisia

[31] Alapuranen (2012), s. 11
[32] Korhonen (2003), s. 83
[33] Saarenpää (2012), s. 328
[34] Saarenpää (2012), s. 328-329
[35] HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi

samantyyppisiä periaatteita kuin nykyisin voimassa olevassa henkilötietolaissa. Tällaisia jo henkilörekisterilaissa säädettyjä periaatteita olivat muiden muassa henkilörekistereissä olevien tietojen tarpeellisuusvaatimus, virheelliseksi havaittujen tietojen oikaisuvelvollisuus, tietojen suojausvelvollisuus sekä rekisteröidyn itseään koskevien tietojen tarkastusoikeus. Henkilörekisterilakia muutettiin useampaan otteeseen sen voimassaoloaikana. Muutoksia tehtiin muiden muassa henkilömatrikkelien laatimista ja sukututkimusta edistävin perustein. Henkilörekisterilain lisäksi tietosuojalainsäädäntöä kehitettiin myös erityislainsäädännöllä.[36] Yksi esimerkki erityislainsäännöstä oli vuonna 1995 säädetty laki poliisin henkilörekistereistä (509/1995).[37]

Tietosuojalainsäädännön historian ja kehityksen kannalta on syytä muistaa myös kansainvälisen sääntelyn merkitys. Yhtenä keskeisimmistä voidaan pitää vuonna 1980 OECD:n antamaa tietosuojasuositusta. Kysymyksessä on lainsäädäntösuositus, joka käsittelee yksityisyyden suojaa ja tiedonsiirtoja maista toisiin. Suosituksessa annetaan ohjeistusta myös rekisteröidyn tarkastusoikeudesta sekä tietoturvasta. Toinen kansainvälisessä mielessä keskeinen henkilötietojen suojaa muovaava tekijä on vuoden 1981 Euroopan neuvoston tietosuojasopimus. Kysymyksessä on yleissopimus, jossa säädellään henkilötietojen automaattisesta tietojenkäsittelystä. Sopimuksella pyritään turvaamaan yksilöille heidän oikeutensa – erityisesti oikeus yksityisyyteen niiden sopimusvaltioiden alueilla, jotka ovat sopimukseen sitoutuneet. Kansainvälisen oikeuden näkökulmasta sopimuksen katsotaan sitovan jäsenvaltioita ja niiden tulee lainsäädännöllä toteuttaa sopimuksessa yksilöille turvatut oikeudet. Molemmalla kansainvälisoikeudellisella asiakirjalla voidaan katsoa olleen keskeinen merkitys vuonna 1995 annettuun henkilötietodirektiiviin ja sitä kautta luonnollisesti myös nykyisin voimassa olevaan henkilötietolakiimme.[38]

2.2 Henkilötietolaki yleislakina

Suomen perusoikeusjärjestelmää nykyaikaistettiin 90-luvun alkupuoliskolla. Uutena säännöksenä mukaan otettiin yksityiselämän suojaa koskeva

[36] Saarenpää (2012), s. 328-329
[37] Alapuranen (2012), s. 12
[38] Korhonen (2003), s. 93-94

säännös.[39] Perustuslain 10.1 § määrää, että jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Lisäksi samaisessa pykälässä säädetään, että henkilötietojen suojasta säädetään tarkemmin lailla.[40] Yksityiselämään voidaan katsoa kuuluvan oikeus olla yksin niin fyysisesti kuin tiedollisessa ja muussa vastaavassa merkityksessä.[41] On syytä kuitenkin myös muistaa, että perustuslaissa suojattua yksityiselämää käsitteenä ei tule ymmärtää liian suppeassa merkityksessä pelkästään yksilön oikeutena olla rauhassa omissa oloissaan vaan myös yksilön oikeutena päättää itse suhteestaan muihin ihmisiin ja ympäristöönsä. Yksityiselämän suojaan voidaan katsoa kuuluvaksi myös oikeus pitää yksityiset asiat omana tietonaan.[42]

Syksyllä 1995 hyväksyttiin Euroopan unionin direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (95/46/EY) (henkilötietodirektiivi). Direktiivi edellytti jäsenvaltioita saattamaan kansallisen tietosuojalainsäädännön direktiivin mukaiseksi kolmen vuoden määräajassa. Suomessa uutta lakia valmistelemaan asetettiin henkilötietotoimikunta. Toimikunta sai työnsä valmiiksi keväällä 1997. Uusi henkilötietojen käsittelyä yleisesti sääntelevä laki, henkilötietolaki, hyväksyttiin eduskunnassa ja se tuli voimaan kesäkuussa 1999 eli kuusi kuukautta myöhässä direktiivissä edellytetystä määräajasta. Voimaan tullessaan henkilötietolaki korvasi aiemman henkilörekisterilain.[43]

Uudella henkilötietojen käsittelyä ohjaavalla lailla haluttiin lisätä rekisteröityjen tiedonsaantioikeuksia. Uudella lailla haluttiin muiden muassa edistää rekisterinpitäjien velvollisuutta antaa oma-aloitteisesti tietoja rekisteröidylle siitä mihin tarkoituksiin rekisteröidyn henkilötietoja käytetään.[44] Tietosuojalainsäädännöllä luodaan perusteet henkilötietojen lailliselle käsittelylle. Yksilöllä pitää lähtökohtaisesti olla päätösvalta siitä milloin ja miten häntä koskevia tietoja käytetään, jollei lainsäädännössä muuta säädetä.[45]

Henkilötietolain 1 § määrittelee lain tarkoituksen:

---

[39] HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta
[40] Koillinen (2013), s. 176
[41] Neuvonen (2013), s. 79
[42] Neuvonen (2008), s. 62
[43] Saarenpää (2001), s. 46-47
[44] HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi
[45] Voutilainen (2009), s. 168

Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Henkilötietolain pääasialliseksi tavoitteeksi voidaan toisin sanoen määritellä tavoite siitä, että henkilötietojen käsittelytoimilla ei rajoiteta yksityiselämän suojaa ja muita perusoikeuksia perusteettomasti ilman laissa säädettyä perustetta. Lain toisena keskeisenä tavoitteena voidaan pitää yhtenäisten hyvään tietojenkäsittelytapaan perustuvien käytäntöjen luomista ja ylläpitämistä.[46]

Henkilötietolaki sovelletaan sen 2 §:n mukaisesti kaikkeen automaattisesti tapahtuvaan henkilötietojen käsittelyyn. Lakia sovelletaan myös manuaaliseen henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai niiden osa. Henkilötielakia ei lähtökohtaisesti sovelleta silloin, jos käsitellään vain yrityksiä ja yhteisöjä koskevia tietoja ja näihin tietoihin ei sisälly henkilötietoja. Henkilötietolaki ei tule myöskään sovellettavaksi silloin, kun yksityinen henkilö käsittelee henkilötietoja yksityisiin tarkoituksiinsa.[47]

Rakenteeltaan henkilötietolaki perustuu pitkälti yleisperiaatteille, joita sovelletaan lähtökohtaisesti kaikissa henkilötietojen käsittelyissä. Tällaisia henkilötietolaissa säädeltyjä yleisperiaatteita ovat esimerkiksi käsiteltävien tietojen tarpeellisuus- ja virheettömyysvaatimus, rekisterinpitäjän suunnittelu- ja huolellisuusvelvollisuus sekä henkilötietoja koskeva käyttötarkoitussidonnaisuuden periaate. Yleisperiaatteiden lisäksi henkilötietolaissa on myös yksityiskohtaisimpia säännöksiä, joita sovelletaan vain määrättyihin erityistilanteisiin.[48] Tällaisia erityissäännöksiä ovat arkaluonteisten henkilötietojen käsittelyn lähtökohtaisesti kieltävät 11 § ja 12 § sekä henkilötunnuksen käsittelyä määrittelevä 13 §.[49] Lisäksi henkilötietolaissa säädetään tietosuojavaltuutetun ja tietosuojalautakunnan asemasta yleisinä henkilötietojen käsittelyjä valvovina viranomaisina.[50]

[46] Alapuranen (2012), s. 44
[47] Salminen (2009), s. 45
[48] Salminen (2009), s. 49-50
[49] Ollila (2002), s. 308
[50] Alapuranen (2012), s. 157, 159

Henkilötietolaki on luonteeltaan yleislaki, jota sovelletaan lähtökohtaisesti aina – muutamia poikkeuksia lukuun ottamatta - silloin kun muussa lainsäädännössä ei toisin säädetä. Määrätyille aloille on säädetty omat erityissäädökset tietosuojasta. Esimerkkinä tällaisista tietosuojan erityislaista voidaan mainita sähköisen viestinnän tietosuojalaki (516/2004) ja laki yksityisyyden suojasta työelämässä (759/2004). Myös moniin muihin lakeihin on otettu erityissäännöksiä koskien henkilötietojen käsittelyä. Aina erityislainsäädännössä ei säädetä aivan kokonaisvaltaisesti henkilötietojen käsittelyyn liittyvistä erityistilanteista, jolloin henkilötietolain säännökset tulevat sovellettavaksi puuttuvilta osin erityislakia täydentäen.[51] Henkilötietoja käsittelevän erityislainsäädännön voitaneen olettaa jäävän pääasiallisesti voimaan myös uuden tietosuoja-asetuksen voimaan saattamisen jälkeen.[52]

3 TIETOSUOJA VERTAILUMAISSA

3.1 Tietosuoja Ruotsissa

Ruotsissa astui voimaan vuonna 1973 maailman ensimmäinen koko valtiota koskenut tietosuojalaki, datalagen (1973:289).[53] Syynä sille, että juuri Ruotsissa säädettiin ensimmäisenä yleinen tietosuojalaki, voidaan ensinnäkin katsoa olleen tietotekniikan voimakas kehitys, joka mahdollisti isojen tietovarantojen nopean sähköisen käsittelyn. Tämän lisäksi, kun otetaan huomioon, että Ruotsissa julkishallinnossa oli – ja on edelleen – vahva julkishallinnolta avoimuutta edellyttävä periaate[54], on selvää, että koettiin että vapaata henkilötietojen käsittelyä tulisi pystyä kontrolloimaan lain tasoisella säädöksellä.[55] Datalagenin säätämisen keskeisenä tavoitteena voidaan katsoa olleen yksilön yksityisyyden suojaaminen ulkopuolelta tapahtuvaa *asiatonta tunkeutumista kohtaan*.[56]

On kuitenkin selvää, että oltuaan voimassa vuosikymmeniä datalagen ei täyttänyt enää niitä vaatimuksia, joita ympäröivä moderni yhteiskunta asetti yksilön yksityisyyden suojalle. Henkilötietodirektiiviin pohjautuen myös

[51] Muttilainen (2006), s. 2
[52] Eklund ja Lilja (2013), s. 220
[53] Syrjänen (2006), s. 40
[54] Muiden muassa vahvaan julkisuusperiaatteeseen vedoten on perusteltu myös oikeutta myydä rikostietoja maksullisessa yksityisesti ylläpidetyssä internetpalvelussa
[55] Seipel (2001), s. 116-117
[56] Korhonen (2003), s. 98

Ruotsissa säädettiin vihdoin vuonna 1998 uusi henkilötietolaki personuppgiftslagen (PuL,1998:204), joka astui voimaan vuonna 2001.[57]

Uuden henkilötietolain sisältöä pohtimaan asetettiin komitea alkuvuodesta 1996. Keskeiseksi kiistakapulaksi komitean sisällä nousi kysymys siitä tulisiko uuden henkilötietolain olla perusperiaatteiltaan sellainen, että kaikenlainen automaattinen henkilötietojen käsittely olisi sallittua paitsi jos se olisi laissa nimenomaisesti kiellettyä. Vai pitäisikö lähtökohtana toisaalta olla periaate, että kaikki automaattiset henkilötietojen käsittelyt ovat lailla säädeltyjä ja jos määrätyn tyyppistä henkilötietojen käsittelyä ei ole laissa sallittu, on se tällöin kiellettyä. Jälkimmäinen tarkkaa sääntelyä vaativa näkökanta voitti, sillä olihan jo vuoden 1973 datalagen pohjautunut tälle ajatukselle. Myös henkilötietodirektiivissä oli sama kaikkeen automaattiseen henkilötietojen säätelyyn tähtäävä periaate, joten uutta henkilötietolakia pohtimaan asetetun komitean työ muodostui lopulta pitkälti direktiivissä annettujen ajatusten kopioimiseksi komitean omaan esitykseen. Hallituksen esitys (1997/98:44) seurasi varsin tarkasti henkilötietolain valmistelua varten asetetun komitean mietintöä ja valtiopäivät hyväksyi esityksen pienin muutoksin uudeksi henkilötietolaiksi.[58]

PuL jäljittelee rakenteeltaan melko pitkälti henkilötietodirektiivin rakennetta. Ensimmäisissä luvuissa valotetaan lain tarkoitusta ja määritellään keskeiset käsitteet. Omat luvut on varattu myös rekisterinpitäjien velvoitteiden määrittelylle, ns. kolmansiin maihin tapahtuvien tietojensiirtojen edellytyksille sekä tietosuojavaltuutetun aseman määrittelylle.[59]

PuL koskee niin julkista kuin yksityistä sektoria. Kun henkilötietoja käsitellään kokonaan tai osittain automaattisin käsittelytoimin, tulee PuL sovellettavaksi yleislakina. Määrätyissä tilanteissa sovelletaan PuL:a myös manuaalisesti suoritettuun henkilötietojen käsittelyyn.[60] PuL määrittelee henkilötietojen käsittelyn käsitteenä kattavan laajasti suuren kirjon erinäisiä henkilötietoihin kohdistuvia toimia. Tällaisina toimina mainitaan muiden muassa henkilötietojen kerääminen, muokkaaminen, varastointi sekä jakaminen. Käsittelytoimien

[57] Regeringskansliet. Personal Data Protection. Information on the Personal Data Act, s. 3-5
[58] Seipel (2001), s. 123-124
[59] Seipel (2001), s. 125
[60] Magnusson Sjöberg (2012), s. 35-39

pääasiallisena perusteena laissa toimii rekisteröidyn suostumus. PuL:n sisältyy myös tietoturvaa koskevia säännöksiä. Myös virheellisten tietojen oikaisua koskevat määräykset on sisällytetty tähän yleisesti sovellettavaan henkilötietosäädökseen.[61]

Henkilötunnuksen käyttöä on PuL:ssa rajoitettu ja sen käytön edellytykseksi on asetettu sen todellisen tarpeen edellytys, esimerkiksi henkilön vahvaa tunnistamista edellyttävä toimi.[62] Tosin jo datalagenissa säädettiin rajoituksia automaattisen tietojen käsittelyn avulla tapahtuvalle henkilötunnuksen käsittelylle.[63] Arkaluonteisten henkilötietojen käsittely on puolestaan PuL:ssa lähtökohtaisesti kielletty. Tähän kieltoon on säädetty tosin useita poikkeuksia. Sallittua on käsitellä arkaluonteisia henkilötietoja esimerkiksi sairaan- ja terveydenhoidonpalveluiden yhteydessä sekä tilastollisia tarkoituksia varten.[64] Rajoituksia on asetettu myös ns. täysin automatisoiduille päätöksentekojärjestelmille. PuL edellyttää, että automatisoituja päätöksentekojärjestelmiä käytettäessä henkilöä, jonka oikeuksia päätös koskee, tulee informoida päätöksentekojärjestelmän käytöstä ja toimintaperiaatteista, joita järjestelmä soveltaa päätöksenteossa.[65]

PuL tekee eron ”jäsennellyn” ja ”jäsentämättömän” henkilötiedon välille. Jäsennellyillä tiedoilla tarkoitetaan henkilötietoja, jotka on kerätty rekisteriin. Sen sijaan, jos henkilötiedot ovat esimerkiksi osana kirjettä tai muuta tekstiä, johon kohdistetaan käsittelytoimia, katsotaan tiedot tällöin jäsentämättömiksi henkilötiedoiksi. Jäsennellyn ja jäsentämättömän henkilötiedon eron määrittelyn merkitys näkyy erityisesti siinä, että jäsenneltyjä henkilötietoja käsitellessä tulee sovellettavaksi useampi PuL:n määräys kuin tilanteissa, joissa käsitellään jäsentämättömiä henkilötietoja.[66]

Kuten sanottua PuL on yleislaki, joten sitä ei sovelleta siltä osin kun erityislaissa on asiasta toisin säädetty. Ruotsissa lukuisissa säädöksissä on omat määräykset koskien henkilötietojen käsittelyjä, jotka eroavat PuL:n vastaavista

[61] Datainspektionen. Ruotsin tietosuojaviranomaisen www-sivut.
Osoitteessa: http://www.datainspektionen.se/
[62] Seipel (2001), s. 143
[63] Öman ja Lindblom (2001), s. 161
[64] Öman ja Lindblom (2001), s. 132-133
[65] Seipel (2001), s. 144
[66] Datainspektionen. Ruotsin tietosuojaviranomaisen www-sivut.
Osoitteessa: http://www.datainspektionen.se/

määräyksistä.[67] Esimerkkeinä tällaisista laista voidaan mainita potilastietolaki patientdatalagen (2008:355), liikennevälineiden rekistereitä koskeva laki ”Lag om vägtrafikregister” (2001:558) sekä sosiaalipalveluissa tapahtuvaa henkilötietojen käsittelyä sääntelevä laki ”Lag om behandling av personuppgifter inom socialtjänsten” (2001:454).[68]

Ruotsissa yleisviranomaisena tietosuojan saralla toimii tietosuojavaltuutettu (Datainspektionen). Tietosuojavaltuutetun toiminnan tärkeimmäksi tavoitteeksi voidaan määritellä lähtökohta, että henkilötietojen tarpeettomalla käsittelyllä ei loukata yksilöiden yksityisyyden suojaa.[69] Ruotsissa tietosuojavaltuutetun toimistossa tätä tavoitetta on nykyisin turvaamassa noin 40 alan asiantuntijaa. Tietosuojavaltuutetun toimiston tehtäviin kuuluu yleisen neuvonnan antaminen, tietosuojaan liittyvän tiedon levittäminen[70] sekä valitusten käsittely. Valitusten käsittely muodostaa keskeisen tehtäväalueen tietosuojavaltuutetun toimiston tehtävistä. Jokainen joka kokee, että hänen oikeuksiaan on loukattu henkilötietojen käsittelyn yhteydessä, voi saattaa vapaamuotoisella valituksella asian tietosuojavaltuutetun käsittelyyn.[71]

Tietosuojavaltuutettu voi myös määrätyissä PuL:ssa määritellyissä tilanteissa antaa erillisohjeita siitä, missä erityistilanteissa henkilötietojen käsittely on sallittua.[72] Lokakuussa 2010 tietosuojavaltuutettu julkaisi tällaisen erillisohjeen, jolla sallittiin yritysten käsitellä henkilötietoja sellaisissa yhteyksissä, joissa tavoitteena on paljastaa yritysten sisäiset lainvastaiset toimet[73], ilman että henkilötietojen käsittelyille tarvitsisi anoa erityislupaa tietosuojavaltuutetulta.[74]

3.2 Tietosuoja Norjassa

Norja oli niiden ensimmäisten valtioiden joukossa, joissa säädettiin tietosuojaa koskeva yleislaki, personregisterloven (1978:48). Tämän varhaisen henkilörekisterilain lähtökohtana oli laaja rekisterinpitäjiä koskeva velvollisuus

[67] Seipel (2001), s. 120
[68] http://www.datainspektionen.se/lagar-och-regler/ovriga-lagar
[69] The Swedish data inspection board. What on earth the data inspection board do? s. 5.
[70] Pääasiallisesti puhelimitse, sähköpostitse ja www.datainspektionen.se – sivuston välityksellä
[71] Datainspektionen. Ruotsin tietosuojaviranomaisen www-sivut.
Osoitteessa: http://www.datainspektionen.se/
[72] Syrjänen (2006), s. 40
[73] Tällaisia järjestelyjä ovat esimerkiksi yritysten työntekijöille tarkoitetut anonyymit vihjelinjat
[74] The Swedish data inspection board. Guidelines for companies. Responsibility for personal data processed in whistleblowing systems.

hankkia etukäteislupa henkilötietojen käsittelytoimille. Oli selvää, että tietotekniikan nopeasti kehittyessä myös henkilötietojen käsittelyn määrä lisääntyi vuosien saatossa valtavasti. Jotta tietosuojaviranomaisten työmäärä ei olisi kasvanut aivan kohtuuttomiin mittoihin, poistettiin vuosien saatossa useita henkilötietojen käsittelytoimia etukäteisluvan vaatimuksen velvoitteesta. Itse henkilörekisterilakia uudistettiin kahdesti vuosina 1987 ja 1993. Uudistuksista huolimatta keskeiset lain periaatteet säilyivät voimassa aina siihen asti kunnes uusi tietosuojaa koskeva yleislaki astui voimaan vuonna 2001[75].[76]

Vaikka Norja ei kuulukaan Euroopan unioniin on se Euroopan talousalueen jäsen (ETA). Täten Norja on pyrkinyt yhtenäistämään lainsäädäntöään unionin säädösten kanssa. Näin myös henkilötietodirektiivin säätämisen innoittamana aloitettiin tietosuojalainsäädännön uudistushanke, joka johti uuden henkilötietolain, personopplysningsloven, voimaan saattamiseen.[77]

Norjan nykyinen henkilötietolaki seuraa ymmärrettävästi sisällöltään pitkälti henkilötietodirektiivin jalanjälkiä, sillä olihan juuri direktiivi keskeinen peruste miksi uutta henkilötietolakia alettiin valmistella. Määrättyjä eroavaisuuksia on kuitenkin havaittavissa näiden kahden säädöksen välillä. Schartum huomauttaa, että henkilötietodirektiivi on kirjoitettu muotoon, jossa tilannekohtaiselle tulkinnalle on jätetty monissa kohdin varsin paljon tilaa. Sen sijaan personopplysningslovenin rakenteessa on nähtävissä määrätynlaiseen yksityiskohtaisuuteen pyrkiminen, jolloin tulkinnalle ei jää samassa mittakaavassa tilaa. Tämän Schartum näkee positiivisena seikkana, sillä yksityiskohtaisella säätelyllä saavutetaan parempi oikeusvarmuus verrattuna siihen jos säädös olisi jätetty yhtä tulkinnanvaraiseksi kuin henkilötietodirektiivi on hänen mielestään jätetty.[78]

Norjalaista juridista tietosuojaa koskevaa ajattelua voidaan nykyisin kuvata käsitteellä ”intressiteoria”.[79] Intressiteorialla voidaan kuvata eri intressejä, joita tietosuojaan liittyy kulloisissakin tilanteissa. Intressiteorian juuret johtavat 1970-luvulle ja erityisesti se vakiinnutti asemansa henkilörekisterilain säätämisen myötä. Teoriaa on kehitetty edelleen vuosikymmenien saatossa lisäämällä

[75] Personopplysningsloven 2000:31
[76] Schartum (2001), s. 79-80, 88
[77] Korhonen (2003), s. 108
[78] Schartum (2001), s. 89-90
[79] Schartum (2001), s. 79

uusia intressejä ja näkökulmia sekä muokkaamalla jo aiemmin kehitettyjen intressikäsitteiden sisältöjä. Keskeistä intressiteorialle on se mikä tarkastelutapa valitaan katsontakannaksi, sillä tämä vaikuttaa keskeisesti siihen mikä intressi tarkastelussa painottuu.[80]

Muiden pohjoismaiden tavoin myös Norjassa on yleinen tietosuojaviranomainen, datatilsynet, joka käsittelee tietosuojaan liittyviä ongelmia. Tämän yleisen tietosuojaviranomaisen tehtäviin kuuluu muiden muassa yleisen tietosuojaan liittyvän neuvonnan antaminen, käytännesääntöjen laatimisessa avustaminen, julkisen rekisterin ylläpitäminen luvan saaneista henkilötietojen käsittelijöistä sekä kansainvälisen juridisen henkilötietojen suojan kehityksen seuraaminen.[81]

3.3 Tietosuoja Yhdysvalloissa

Yhdysvalloissa ei ole säädetty yksityisyyslakia, joka kattaisi kaikki yksityisyyteen liittyvät tilanteet. Lähtökohtana sen sijaan on perinteisesti ollut, että yksityisyyteen liittyviin ongelmiin on pyritty puuttumaan yksittäistapauksina sitä mukaa, kun niitä on noussut esille.[82]

Yhdysvaltain perustuslaista voidaan nostaa esille kohtia, joiden voidaan katsoa suojaavan muiden oikeuksien ohella myös yksilön oikeutta yksityisyyteen. Tällöin nimenomaan on kysymys yksilön suojasta suhteessa liittovaltion oikeudetonta yksityisyyteen puuttumista vastaan. Yksi keskeisimmistä kohdista, jonka on katsottu suojaavan yksityisyyttä, on perustuslain 4. lisäys. Siinä suojataan kansalaisia kieltämällä perusteettomat kotietsinnät ja muut henkilön omaisuuteen kohdistuvat tutkimukset. Perustuslakia tulkittaessa keskeisenä suunnan näyttäjänä toimii liittovaltion korkein oikeus (US supreme court). Korkeimman oikeuden päätöksissä perustuslain 4. lisäystä on tulkittu siten, että sen on katsottu antavan yksilölle oikeuden odottaa ns. kohtuullisen tason yksityisyyttä (reasonable expectation of privacy). Myös perustuslain 14. lisäyksen, joka määrää oikeudenmukaisesta ja tasavertaisesta

[80] Korhonen (2003), s. 103-104
[81] Datatilsynet. Norjan tietosuojaviranomaisen www-sivut. Osoitteessa: http://www.datatilsynet.no/
[82] Syrjänen (2006), s. 44

lainkäyttöprosessista, on katsottu lukuisissa korkeimman oikeuden ratkaisussa[83] turvaavan oikeuden yksityisyyteen.[84]

Vaikka Yhdysvalloissa ei olekaan ns. yleistä henkilötietolakia, joka kattaisi yleisesti kaikki yksityisyyteen liittyvät tilanteet, on liittovaltiotasolla säädetty kaksi keskeistä lakia, joilla ohjataan henkilötietojen käsittelyä ja niiden luovutuksia: Privacy Act[85] ja Freedom of information act[86]. Kummassakin laissa säädetään henkilötietoihin liittyvistä seikoista, mutta Freedom of information act on keskittynyt erityisesti vapaan tiedon saannin turvaamiseen. Molemmat lait on tarkoitettu ensisijaisesti ohjaamaan julkishallinnon henkilötietojen käsittelyä. Privacy act edellyttää, että henkilötietoja kerätään ja käsitellään vain silloin kun se on tarpeellista. Lisäksi henkilötiedot on ensisijaisesti kerättävä rekisteröidyltä itseltään ja myös riittävästä tietoturvan tasosta on huolehdittava.[87]

Yksityisellä sektorilla puolestaan on alakohtaista sääntelyä, jonka luonne ja yksityisyydelle tarjoama suoja saattavat vaihdella huomattavastikin alasta riippuen. Bygrave pitää syynä siihen, että yleistä tietosuojalakia ei ole saatu aikaiseksi Yhdysvalloissa, yksityisen sektorin skeptistä asennoitumista tähän tavoitteeseen. Yksityinen sektori on halunnut pitää markkinatalouden mahdollisimman vapaana valtiovallan taholta annetusta sääntelystä – näin myös henkilötietojen käsittelyä koskevan lainsäädännön osalta. On varsin selvää, että sektorikohtaisten yksityisyyssäädösten vaihtelevuudesta johtuen vallitseva tilanne ei yksityisyyden suojan kannalta katsottuna ole riittävä.[88]

Yhdysvaltojen ja Euroopan unionin alueen välisten henkilötietojen siirtojen sujumisen varmistamiseksi Yhdysvalloissa on otettu käyttöön ns. safe harbor-järjestelmä. Safe harbor-järjestelmässä syntyi sen seurauksena, että unionin komissio katsoi, että Yhdysvaltain lainsäädäntö ei tarjoa riittävää henkilötietojen suojaa, jotta henkilötietojen siirrot Yhdysvaltoihin voitaisiin unionin alueelta sallia. Lähinnä sujuvien kauppasuhteiden varmistamiseksi tarvittiin järjestelmä, jolla henkilötietojen siirrot pystyttäisiin toteuttamaan, samalla kuitenkin varmistaen riittävä henkilötietojen suojan tason toteutuminen. Komissio ja

[83] Esimerkiksi tapaus Roe v. Wade, 410 U.S. 113, 1973
[84] Syrjänen (2006), s. 45
[85] 5 U.S.C. § 552a, 1974
[86] 5 U.S.C. § 552, 1966
[87] Syrjänen (2006), s. 46
[88] Bygrave (2002), s. 54-55

Yhdysvaltojen kauppaministeriö ovat yhteisesti hyväksyneet luettelon periaatteista, joita noudattamalla organisaation katsotaan takaavan riittävä henkilötietojen suojan taso (komission päätös: 2000/520/EY).[89]

Safe harbor-periaatteisiin kuuluu rekisterinpitäjän velvollisuus informoida yksityishenkilöä siitä, mihin tarkoitukseen henkilötietoja kerätään ja miten kerättyjä henkilötietoja käytetään sekä velvollisuus järjestää henkilölle mahdollisuus tarkistaa itseään koskevat tiedot ja tietojen osoittautuessa virheelliseksi velvollisuus korjata tai poistaa virheelliset tiedot. Yhdysvaltojen kauppaministeriö pitää julkista luetteloa organisaatioista, jotka ovat sitoutuneet noudattamaan safe harbor-periaatteita.[90] Lähinnä järjestelyn vapaaehtoisuudesta johtuen on esitetty epäilyksiä sen käytännön juridisesta sitovuudesta ja siitä onko ratkaisu pitkällä aikavälillä oikea valinta turvallisille henkilötietojen siirroille mantereiden välillä.[91]

Perinteisesti Yhdysvalloissa on ajateltu, että juridisille henkilöille ei ole taattu lainsäädännössä samanlaista oikeutta yksityisyyteen kuin yksityisille henkilöille. Oikeuskäytännössä yhteisenä tulkintalinjana on ollut, että sitä yksityisyyden suojaa, jota sovelletaan yksityisiin henkilöihin, ei voida suoraan soveltaa yrityksiin. Oikeuskäytännössä lähtökohtana on ollut, että yritykset eivät voi nostaa oikeusjuttuja sillä perusteella, että heidän yksityisyyttään olisi loukattu. Oikeuskäytäntö ei kuitenkaan ole täysin sulkenut pois yrityksiltä oikeutta joihinkin yksityisyyteen liittyviin osa-oikeuksiin. Tästä esimerkkinä voidaan mainita monessa oikeustapauksessa[92] hyväksytty periaate siitä, että myös yritykset nauttivat suojaa perustuslain 4. lisäyksen mukaisesti perusteettomilta kotietsinnöiltä ja muilta omaisuuteen kohdistuvilta tutkimuksilta. [93]

---

[89] Euroopan unionin komission lehdistötiedote. Tietosuoja: komissio tukee Yhdysvaltojen kanssa tehtävää "safe harbor" –sopimusta.
Osoitteessa: http://europa.eu/rapid/press-release_IP-00-301_fi.htm

[90] Tietosuojavaltuutetun toimisto. Yhdysvaltalainen Safe Harbor-järjestelmä.
Osoitteessa: http://www.tietosuoja.fi/25914.htm

[91] Bygrave (2002), s. 83

[92] Esimerkiksi tapaus G M Leasing v. United States, 429 US 338,353, 1977

[93] Bygrave (2002), s. 192-194

4 REKISTERINPITÄJÄN YLEISET VELVOLLISUUDET

4.1 Rekisterinpitäjän vastuu sekä sisäänrakennettu ja oletusarvoinen tietosuoja

Asetusehdotuksen 22 artikla velvoittaa rekisterinpitäjän järjestämään toimintansa siten, että tämän asetuksen rekisterinpitäjille asettamat velvoitteet toteutuvat. Artiklan toisessa kohdassa määritellään mitä nämä toimet käytännössä voivat olla. Näihin yleisiin velvoitteisiin lasketaan kuuluvaksi tietoturvallisuutta koskevien vaatimusten toimeenpano, tietosuojavastaavan nimittäminen sekä ennakkohyväksyntää tai ennakkokuulemista edellyttävien säännösten noudattaminen. Artiklan sanamuodosta käy selvästi ilmi, että kysymyksessä ei suinkaan ole tyhjentäväksi tarkoitettu listaus toimenpiteistä, joilla rekisterinpitäjä voi järjestää toimintansa tämän asetuksen mukaiseksi. Myös muunlaisilla toimilla voidaan ja tuleekin täyttää tämän asetuksen tarkoitusten toteutuminen. Tämän lisäksi artiklassa edellytetään, että rekisterinpitäjän on toteutettava toimet, joilla rekisterinpitäjän velvoitteiden tehokas toteutuminen pystytään varmentamaan. Tällaisina toimina pidetään riippumattomia organisaation sisäisiä ja ulkoisia tarkastuksia.

Asetusehdotuksen yksityiskohtaisissa perusteluissa viitataan 22 artiklan osalta ns. tilivelvollisuuden periaatteeseen. Tilivelvollisuudella tarkoitetaan sitä, että rekisterinpitäjän pitää pystyä osoittamaan se, että jokaisessa tietojen käsittelyn vaiheessa on noudatettu lakia. Käytännössä tämä tarkoittaa sitä, että kaikista henkilötietojen käsittelytoimista tulee jäädä dokumentteihin merkintä. Merkintöjä tarkastelemalla tulee sekä rekisterinpitäjän itsensä että myös ulkopuolisen tahon pystyä varmentamaan se, että henkilötietojen käsittelyt on suoritettu lainmukaisesti.[94]

Asetusehdotuksen 23 artikla edellyttää, että rekisterinpitäjä toteuttaa sellaiset *tekniset ja organisatoriset toimenpiteet*, joilla pystytään varmistamaan asetusehdotuksen edellyttämien henkilötietojen suojaa koskevien vaatimusten toteutuminen. Tätä vaatimusta artiklassa vielä edelleen tarkennetaan määräämällä rekisterinpitäjän oletusarvoksi toimintatapa, jossa käsittelyn kannalta kerätään vain se määrä henkilötietoja kuin käsittelyn kannalta on

[94] Männikkö (2012), s. 28-30

tarpeellista. Kerättyjä tietoja ei tämän periaatteen mukaisesti myöskään saa säilyttää yhtään sen pidempää kuin se on käsittelyn kannalta välttämätöntä.

Lisäksi näihin ns. oletusarvoisiin organisaation sisäänrakennetun tietosuojan vaatimuksiin katsotaan kuuluviksi sellaiset toimintatavat, joilla varmistetaan ettei kaikilla henkilötietoja käsittelevässä organisaatiossa työskentelevillä ole rajatonta pääsyä henkilötietoihin. Toisin sanoen, kun henkilötietoja käsitellään, vain niillä, jotka osallistuvat henkilötietojen käsittelyyn saa olla organisaatiossa pääsy käsittelyn kannalta tarpeellisiin henkilötietoihin. Artiklan 23 kolmannessa ja neljännessä kohdassa annetaan komissiolle valta säätää säädöksiä, joissa määritellään yksityiskohtaisemmin mitä edellä käsitellyillä sisäänrakennetuilta ja oletusarvoisilta vaatimuksilla kulloinkin käytännön tasolla vaaditaan sekä oikeus yksityiskohtaisemmin vahvistaa näitä koskevat tekniset standardit.

4.2 Henkilötietolain yleisiä periaatteita koskien rekisterinpitäjän toiminnan järjestämistä

Henkilötietolaista voidaan nostaa esille kaksi keskeistä rekisterinpitäjän toiminnan järjestämistä ohjaavaa periaatetta: 5 §:n huolellisuusvelvoite ja 6 §:n suunnitteluvelvoite.[95]

Henkilötietolain 5 §:ssä säädetään rekisterinpitäjän huolellisuusvelvoitteesta. Rekisterinpitäjän tulee henkilötietojen käsittelyssään toimia lain mukaisesti sekä huolellisesti ja hyvän tietojenkäsittelytavan mukaisesti. Kaiken toiminnan tulee myös olla sellaista, että rekisteröidyn yksityiselämän suojaa ja yksityisyyden suojaavia perusoikeuksia ei rajoiteta ilman lain mukaisia perusteita. Samat velvoitteet koskevat pykälän mukaan myös niitä, jotka itsenäisinä elinkeinon- tai toiminnanharjoittajina toimivat rekisterinpitäjän lukuun.[96]

Henkilötietolain 5 § asettaa rekisterinpitäjälle velvollisuuden oma-aloitteisesti huolehtia siitä, että huolellisuusvelvoitteeseen sisältyvät tavoitteet toteutuvat. Toisin sanoen rekisterinpitäjän on järjestettävä toimintansa siten, että henkilötietojen käsittelyssä otetaan huomioon rekisteröidyn yksityisyyttä koskevat säännökset. Käytännön tasolla tällaisilla toimilla tarkoitetaan esimerkiksi sitä, että henkilötietoja käsitteleville työntekijöille on järjestettävä

[95] Aarnio (2012), s. 3
[96] Alapuranen (2012), s. 79

riittävä tietosuojalainsäädäntöä koskeva koulutus. Henkilötietojen käsittelyä koskeva toiminta on muutenkin järjestettävä siten, että siinä käytetyt menettelytavat ottavat huomioon lainsäädännön vaatimukset.[97]

Rekisterinpitäjän huolellisuusvelvollisuus voidaan nähdä tärkeänä rekisterinpitäjää koskevana yleisperiaatteena, jonka tärkeyttä lainsäätäjä on erityisesti halunnut painottaa 5 §:n ensimmäisessä virkkeessä: *rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti* jne. Alapuranen on erityisesti kiinnittänyt tähän huomiota, sillä hänen mukaansa ei ole kovinkaan yleistä, että itse lainsäädännössä erityisesti käskettäisiin noudattamaan lakia koska lait jo itsessään pitävät sisällään luontaisen ajatuksen niiden noudattamisesta. Voidaankin perustellusti kysyä miksi näin kuitenkin on 5 §:ssä toimittu. Alapuranen näkee asian siten, että laillisuutta korostavalla viittauksella on haluttu viitata tietojenkäsittelijän ja rekisteröidyn väliseen suhteeseen. Tällöin yksityisyyden suojan sisältö määräytyy sen mukaisesti millainen tämä suhde on. Toisin sanoen laillisuutta koskeva viittaus voidaan ymmärtää hänen mukaansa lainsäätäjän määrittelynä tilanteesta, jossa toisen yksityisen tahon oikeus tai edut muodostavat syyn henkilötietojen käsittelylle silloin, kun kysymys on yksilön tahdosta riippumattomasta henkilötietojen käsittelystä.[98]

Toisaalta on esitetty myös muunlaisia perusteluita sille, miksi henkilötietolain 5 §:ssä lain noudattamista halutaan erityisesti painottaa. Raatikainen näkee asian siten, että laillisuuspainotuksella viitataan muun lainsäädännön noudattamiseen. Hänen mukaansa lainsäätäjä on halunnut painottaa, että huolellisuusvelvoitetta toteuttaessaan rekisterinpitäjän tulee huolehtia myös muussa lainsäädännössä asiasta säädetyn noudattamisesta. Tällainen tilanne voi olla käsillä esimerkiksi silloin, kun henkilötietolain lisäksi määrätystä seikasta säädetään myös erityislainsäädännössä.[99]

Kolmas perustelu laillisuutta korostavalle painotukselle on Nyyssölän ajatus siitä, että virkkeellä on haluttu painottaa lain noudattamisen vaatimusta siitä yksinkertaisesta syystä, että henkilötietojen suojaa koskeva lainsäädäntö oikeudenalana on vielä suhteellisen nuorta. Henkilötietojen suojaa koskevan lainsäädännön uutuudesta johtuen siihen ei aina ole välttämättä suhtauduttu

[97] Alapuranen (2012), s. 79
[98] Alapuranen (2012), s. 79-80
[99] Raatikainen (2002), s. 71

samalla lakia kunnioittavalla asenteella kuin sellaiseen lainsäädäntöön, jolla on jo vakiintunut asema.[100]

Henkilötietojen käsittelyn suunnitteluvelvoitteesta säädetään henkilötietolain 6 §:ssä. Henkilötietojen käsittelyn tulee ensinnäkin olla asiallisesti perusteltua rekisterinpitäjän toiminnan kannalta katsottuna. Henkilötietojen käsittelyn järjestäminen on suunniteltava ennalta ennen varsinaisen henkilötietojen käsittelyn aloittamista. Suunnitelmallisuus koskee koko henkilötietojen käsittelyä koskevaa prosessia. Suunnittelussa huomioon on otettava henkilötietojen käsittelyn tarkoitukset sekä se, mistä henkilötiedot hankitaan ja mihin niitä mahdollisesti luovutetaan. Lisäksi suunnittelussa tulee ottaa huomioon myös henkilötietojen varsinaiset käsittelytoimet, käyttötarkoitukset, säilytys, arkistoihin siirtämiset sekä lopuksi niiden hävittäminen. Henkilötietojen käsittelyn tulee olla tiettyä tai tiettyjä käyttötarkoituksia varten rajattua toimintaa. Lain mukaista ei ole toiminta, jossa kerätään henkilötietoja ja jätetään käyttötarkoitus avoimeksi, vasta tulevaisuudessa päätettäväksi seikaksi.[101]

Henkilötietojen käyttötarkoitus tulee määritellä siten, että siitä käy ilmi, minkälaisten rekisterinpitäjien tehtävien hoitamiseksi henkilötietoja käsitellään. Voidaan ajatella, että toiminnan tosiasiallisen suunnitelmallisuuden lisäksi toiminnan tulee myös näyttää ulospäin katsottuna suunnitelmallisesti. Toisin sanoen henkilötietojen käsittelyn suunnitelmallisuudella voidaan nähdä olevan yhteys myös avoimuuden periaatteeseen. Tätä avoimuutta toteutetaan muiden muassa henkilötietolain 10 §:ssä määritellyllä rekisteriselosteella, jonka on lähtökohtaisesti oltava aina kaikkien saatavilla.[102]

Saarenpää muistuttaa, että laiminlyömällä suunnitteluvelvoite ei pystytä välttymään tietosuojalainsäädännön rekisterinpitäjälle asettamilta velvoitteilta. Toisin sanoen esimerkiksi tilanteessa, jossa tosiasiallisesti käsitellään yhteistä tarkoitusta varten henkilötietoja sisältäviä asiakirjoja, ja vaikka toimintaa ei ole ennalta suunniteltu, niin kysymyksessä on tietosuojalainsäädännön kannalta katsottuna henkilörekisteri.[103]

---

[100] Nyyssölä (2009), s. 39-40
[101] Saarenpää (2012), s. 345-346
[102] Saarenpää (2012), s. 345-346
[103] Saarenpää (2012), s. 345

4.3 Yhteiset rekisterinpitäjät

Asetusehdotuksen 24 artiklassa määritellään tilanne, jossa useampi rekisteripitäjä toimii yhdessä siten, että ne määrittelevät *henkilötietojen käsittelyn tarkoitukset, edellytykset ja keinot yhdessä*. Tämän voidaan siis ajatella tarkoittavan tilannetta, jossa useammat rekisterinpitäjät toimivat yhteiseen lukuun määrätyn tavoitteen saavuttamiseksi. Tällöin henkilötietojen käsittelyn toimintametodit ja tavoitteet määritellään ja toteutetaan yhdessä yhteisen päämäärän saavuttamiseksi. Tämän asetuksen velvoitteiden toteuttamiseksi ja erityisesti rekisteröidyn oikeuksien käyttämisen turvaamiseksi jokaiselle toimijalle on vahvistettava oma vastuualue. Se miten vastuualueet jaetaan on jätetty rekisterin keskinäisten toimijoiden päätettäväksi.

4.4 Yhteiset rekisterinpitäjät henkilötietolaissa

Henkilötietolaissa ei ole erityistä asetusehdotuksen 24 artiklan kaltaista määräystä vastuualueiden määräämisestä yhteisrekisterinpitäjille. Henkilötietolain 3 §:n 4 kohdassa määritellään rekisterinpitäjän käsite. Sanamuodosta voidaan suoraan lukea, että yhdeksi rekisterinpitäjäksi voidaan määritellä samanaikaisesti yksi tai useampi järjestelyssä mukana oleva taho. Näin ollen henkilötietolakiin voidaan katsoa sisältyvän jo lähtökohtana ajatus siitä, että rekisterinpitäjä voi muodostua useammasta luonnollisesta henkilöstä tai oikeushenkilöstä. Keskeisenä seikkana määriteltäessä rekisterinpitäjä-käsitettä voidaan nähdä se, kenellä tai keillä on oikeus määrätä henkilörekisterin käytöstä. Esimerkkinä tilanteesta, jossa rekisterinpitäjän voidaan katsoa muodostuvan useammasta toimijasta, voidaan mainita matkavarausjärjestelmä, joka muodostuu matkatoimistojen, lentoyhtiöiden ja hotellien varausjärjestelmistä.[104]

Henkilötietolain soveltamislaajuuden kannalta on kuitenkin myös syytä pitää mielessä, että lakia sovelletaan kaikkeen automaattisesti suoritettavaan henkilötietojen käsittelyyn. Tällöin lain soveltamisen kannalta välttämätöntä ei ole, että olemassa olisi rekisterinpitäjä ja henkilörekisteri. Myös muu toimija kuin rekisterinpitäjäksi miellettävä taho joutuu tällaisissa automaattisen

[104] Vanto (2011), s. 30-31

henkilötietojen käsittelyiden tilanteissa toimimaan henkilötietolain velvoitteiden mukaisesti.[105]

4.5 Unionin ulkopuolelle sijoittautuneiden rekisterinpitäjien edustajat

Artiklassa 25 säädetään tilanteista, joissa rekisterinpitäjä sijaitsee Euroopan unionin ulkopuolella. Tällöin rekisterinpitäjällä on määrätyissä tilanteissa velvollisuus nimittää edustaja unionin alueella tapahtuvaa toimintaansa varten.[106] Edustajan on sijaittava jossakin niistä jäsenvaltioista, missä rekisteröidyt asuvat. Edustajan nimittäminen ei poista oikeutta aloittaa niitä oikeustoimia, jotka voitaisiin lain mukaan muutenkin rekisterinpitäjää vastaan kohdistaa.

Edustajan nimittämisvelvollisuutta ei artiklan mukaan kuitenkaan sovelleta seuraaviin tahoihin:

a) rekisterinpitäjään, joka on sijoittautunut sellaiseen kolmanteen maahan, jonka tarjoamaa tietosuojan tasoa komissio pitää riittävänä 41 artiklan mukaisesti; tai

b) yritykseen, jossa on alle 250 työntekijää; tai

c) viranomaisiin ja julkishallinnon elimiin; tai

d) rekisterinpitäjään, joka tarjoaa tavaroita tai palveluja unionin alueella asuville rekisteröidyille vain satunnaisesti.

4.6 Suomen lain soveltaminen ja edustajat

Henkilötietolain 4 §:ssä säädetään Suomen lain soveltamisesta. Sen mukaisesti henkilötietolakia sovelletaan silloin kun rekisterinpitäjän toimipaikka sijaitsee Suomen alueella tai ”muutoin Suomen oikeudenkäytön piirissä”. Esimerkkinä toimipisteestä, jonka voidaan katsoa olevan Suomen oikeudenkäytön piirissä, voidaan mainita Suomen ulkomailla sijaitseva diplomaattinen edustusto.[107]

Henkilötietolain 4 §:ssä määrätään, että tilanteissa joissa rekisterinpitäjä, jolla ei ole toimipaikkaa minkään unionin jäsenvaltion alueella ja joka käyttää Suomessa sijaitsevia laitteita henkilötietojen käsittelyyn, joutuu nimittämään Suomeen itselleen edustajan. Tällöin edellytyksenä on, että laitteita käytetään

[105] Alapuranen (2012), s. 46
[106] Artiklan 3 toisen kohdan mukaisesti
[107] Vanto (2011), s. 36

muuten tietojen käsittelyyn kuin vain pelkästään tietojen siirtoon Suomen kautta. Sen määrittäminen, milloin kysymyksessä on vain tietojen siirtoa koskeva toimi, ei välttämättä ole aina kovin helppoa ja yksiselitteistä.[108]

Tietosuojatyöryhmä on antanut useita lausuntoja tilanteista, joissa on ollut vaikeuksia määrittää käyttääkö rekisterinpitäjä unionin alueella sijaitsevaa laitetta henkilötietojen käsittelyyn.[109] Vuodelta 2002 peräisin olevassa lausunnossa otetaan kantaa sellaisten nettisivujen toimintaan, jotka toimivat unionin ulkopuolelta käsin. Tällöin keskeisiksi seikoiksi on katsottu rekisterinpitäjän mahdollisuus ja tarkoitus käyttää unionin alueelle sijoittunutta laitetta. Esimerkkinä tällaisesta tilanteesta mainitaan tilanteet, joissa unionin ulkopuolella toimivan nettisivun kautta käyttäjän koneelle asetetaan ns. *cookie* eli *eväste*, jonka avulla käyttäjälle voidaan kohdistaa yksilöllistä mainontaa. Tällöin, kun tietokone sijaitsee unionin alueella, tulee tilanteeseen sovellettavaksi unionin jäsenvaltion kansallinen lainsäädäntö eli esimerkiksi Suomessa henkilötietolaki.[110]

4.7 Henkilötietojen käsittelijä sekä tietojenkäsittely rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa

Asetusehdotuksen 26 artiklassa määritellään käsite ”henkilötietojen käsittelijä”. *Henkilötietojen käsittelijällä* tarkoitetaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Artiklassa asetetaan yleiset standardit henkilötietojen käsittelijälle. Henkilötietojen käsittelijän tulee antaa *riittävät takeet* siitä, että henkilötietoja käsitellään siten, että käsittelyyn liittyvät toimet toteutetaan niin, että ne täyttävät asetusehdotuksen käsittelylle asettamat vaatimukset. Tällöin sekä teknisten toimien että myös henkilötietojen käsittelijän organisaatioon liittyvien ominaisuuksien on täytettävä nämä velvoitteet. Artiklassa lisäksi edellytetään, että sovittujen velvoitteiden noudattamista valvotaan. Komissiolle

[108] Tietosuojatyöryhmän lausunto: Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30. toukokuuta 2002, www.ec.europa.eu/justice
[109] Vanto (2011), s. 37
[110] Tietosuojatyöryhmän lausunto: Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, 30. toukokuuta 2002, www.ec.europa.eu/justice

annetaan oikeus säätää tarkempia säädöksiä koskien edellä mainittuja takeita ja standardeja.[111]

Artiklan toisessa kohdassa määrätään, että rekisterinpitäjän ja henkilötietojen käsittelijän välille on tehtävä sopimus[112], jossa määritellään henkilötietojen käsittelyn sisältö. Tässä sopimuksessa on erityisesti sovittava seuraavista seikoista:

a) toimii ainoastaan rekisterinpitäjän ohjeiden mukaisesti, etenkin jos käsiteltäviä henkilötietoja ei saa siirtää;

b) ottaa palvelukseen ainoastaan sellaista henkilöstöä, joka on sitoutunut noudattamaan salassapitovelvollisuutta tai jota koskee lakisääteinen salassapitovelvollisuus;

c) toteuttaa kaikki 30 artiklassa vaaditut toimenpiteet;

d) käyttää toisen henkilötietojen käsittelijän palveluksia vasta rekisterinpitäjän ennakkohyväksynnän saatuaan;

e) käsittelytoimen luonteen salliessa laatii yhdessä rekisterinpitäjän kanssa tarvittavat tekniset ja organisatoriset vaatimukset, jotta voidaan täyttää rekisterinpitäjän velvollisuus vastata pyyntöihin, jotka koskevat III luvussa säädettyjen rekisteröidyn oikeuksien käyttämistä;

f) auttaa rekisterinpitäjää varmistamaan, että 30–34 artiklassa säädettyjä velvollisuuksia noudatetaan;

g) luovuttaa käsittelyn päätyttyä kaikki tulokset rekisterinpitäjälle eikä enää muutoin käsittele kyseisiä henkilötietoja;

h) toimittaa rekisterinpitäjälle ja valvontaviranomaiselle kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen valvontaa varten.

Poimintana edellä mainituista voidaan esille nostaa kohta b, jossa velvoitetaan henkilötietojen käsittelijä käyttämään henkilötietojen käsittelyssä *ainoastaan sellaista henkilöstöä, joka on sitoutunut noudattamaan salassapitovelvollisuutta tai jota koskee lakisääteinen salassapitovelvollisuus*. Tällöin on selvää, että tällainen sopimusklausuuli luo henkilötietojen käsittelijälle eräänlaisen jatkovelvoitteen järjestää oman henkilöstöorganisaationsa siten, että kaikki henkilöt, jotka osallistuvat henkilötietojen käsittelyyn, ovat solmineet salassapitosopimuksen. Toisaalta tämän perusteen riittäväksi toteutumiseksi katsotaan asetusehdotuksen artiklassa myös se, jos lain perusteella syntyy tällainen salassapitovelvoite kyseisenlaisissa tilanteissa – toisin sanoen salassapitovelvoitteesta ei tällöin tarvitse lisäksi sopia sopimusvelvoittein.

[111] 86 artiklan mukaisesti
[112] tai muu *oikeudellinen asiakirja*

Artiklan neljännessä kohdassa määrätään, että jos henkilötietojen käsittelijä alkaakin käsitellä muita kuin rekisterinpitäjän hänelle määräämiä henkilötietoja, niin tällöin henkilötietojen käsittelijää pidetään näiden muiden tietojen käsittelyn osalta rekisterinpitäjänä. Tällöin sovellettavaksi tulevat 24 artiklan säännökset yhteisistä rekisterinpitäjistä.

Asetusehdotuksen 27 artiklassa määrätään kiellosta käsitellä henkilötietoja rekisterinpitäjän ohjeiden vastaisesti. Tällä kiellolla tarkoitetaan niin henkilötietojen käsittelijää kuin hänen tai rekisterinpitäjän alaisuudessa toimivia henkilöitä. Poikkeustilanteiksi on kuitenkin säädetty tapaukset, joissa unionin tai kansallisen lainsäädännön säädökset velvoittavat rekisterinpitäjän ohjeiden vastaiseen tietojen käsittelyyn.

4.8 Asiakirjat

Artiklassa 28 säädetään henkilötietojen käsittelyssä syntyvistä asiakirjoista ja niiden säilyttämisestä. Artiklassa velvoitetaan niin rekisterinpitäjä kuin henkilötietojen käsittelijä sekä heidän edustajansa säilyttämään kaikista heidän suorittamistaan henkilötietojen käsittelyistä syntyneet asiakirjat.

Artiklan toisessa kohdassa määritellään minimivaatimustasot henkilötietojen käsittelyissä syntyvien asiakirjojen sisällöille. Asiakirjoissa on oltava vähintään a.) henkilötietojen käsittelijän nimi sekä yhteystiedot, b.) jos organisaatiossa on tietosuojavastaava, niin hänen nimi ja yhteystiedot, c.) henkilötietojen käsittelyn tarkoitusperusteet, d.) kuvaus rekisteröityjen ryhmittelystä ja kuvaus näiden ryhmittelyjen sisällöistä, e.) tahot joille henkilötietoja kulloinkin luovutettu eli henkilötietojen vastaanottajat, f.) tieto siitä, jos henkilötietoja on siirretty kolmansiin maihin tai kansainvälisille järjestöille, g.) tieto kunkin tietoryhmän poistamisen määräajoista, h.) tieto 22 artiklan edellytysten toteutumisen valvonnasta eli ts. menetelmistä, joilla ko. edellytysten toteutumista on kulloinkin valvottu.

Asiakirjojen säilyttämisvelvoitteesta ja asiakirjojen minimivaatimusvelvoitteista on asetusesityksen mukaan kuitenkin vapautettu yksityiset henkilöt, jotka käsittelevät henkilötietoja toiminnassa, jonka tarkoituksena ei ole kaupallinen toiminta sekä lisäksi yritykset, joilla on alle 250 työntekijää. Yritysten kohdalla lisäedellytyksenä on, että yritys käsittelee henkilötietoja *ainoastaan*

pääasiallisen toimintansa aputoimintona. Tällä tarkoitettaneen sitä, että edellä mainituista velvoitteista voidaan tällöin vapauttaa vain sellaiset yritykset, joiden liiketoiminta ei ole henkilötietojen käsittely kaupallisena toimintana, vaan henkilötietoja käsitellään vain silloin, kun tähän on pääasiallisen liiketoiminnan takia tarvetta, esimerkiksi henkilötietojen käsittely asiakkaitten tilausten käsittelyn yhteydessä.

Tahon, jonka edellä olevan mukaisesti on tuotettava henkilötietojen käsittelystään asiakirjat, on pyydettäessä esitettävä kyseiset asiakirjat valvontaviranomaiselle. Artiklassa annetaan lisäksi komissiolle valta säätää tarkempia säädöksiä koskien henkilötietojen käsittelyssä syntyviä asiakirjoja. Komissio voi tätä tarkoitusta varten vahvistaa käytettävät vakiolomakkeet.

4.9 Yhteistyö valvontaviranomaisen kanssa

Asetusehdotuksen 29 artiklassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän sekä heidän edustajiensa velvollisuudesta tehdä yhteistyötä valvontaviranomaisen kanssa. Erityisesti artiklassa viitataan saman asetusehdotuksen 53 artiklan toisessa kohdassa asetettujen edellytysten täyttämiseen.

53 artiklan toinen kohta:

Jokaisella valvontaviranomaisella on tutkintavaltuudet saada rekisterinpitäjältä tai henkilötietojen käsittelijältä:

a) pääsy kaikkiin henkilötietoihin ja kaikkiin tietoihin, jotka ovat tarpeen sen tehtävien suorittamista varten;

b) pääsy kaikkiin sen tiloihin, tietojenkäsittelylaitteet ja -keinot mukaan lukien, jos on kohtuulliset perusteet olettaa, että siellä suoritetaan tämän asetuksen vastaista toimintaa.

Edellä b alakohdassa tarkoitettuja valtuuksia on käytettävä unionin ja jäsenvaltion lainsäädännön mukaisesti.

Artiklan 29 toisessa kohdassa määrätään vielä tarkemmin edellä mainittujen velvoitteiden täyttämisestä. Valvontaviranomainen määrittää kohtuullisen ajan, jonka kuluessa rekisterinpitäjän ja henkilötietojen käsittelijän on vastattava 53 artiklan 2 kohdan nojalla esitettyihin pyyntöihin. Vastaukseen on sisällytettävä valvontaviranomaisen huomautusten pohjalta tehdyt toimenpiteet sekä selvitykset näiden pohjalta syntyneistä tuloksista.

5 TIETOTURVA

5.1 Käsittelyn turvallisuus

Artiklassa 30 säädetään rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudesta toteuttaa toimet, joilla varmistetaan henkilötietojen käsittelyn *asianmukainen turvallisuustaso*. Toimilla tarkoitetaan tässä yhteydessä niin teknisiä kuin organisatorisia toimenpiteitä. Artiklan mukaan turvallisuustasoa määritettäessä otetaan huomioon käytettävissä oleva uusin tekniikka sekä toimien toteuttamisesta aiheutuvat tekniset kustannukset. Lisäksi arvioinnissa tulee ottaa huomioon kulloinkin käsillä oleville henkilötiedoille tyypilliset riskit.

Artiklan toisessa kohdassa määritellään millaisilta uhilta ensimmäisen kohdan toimilla pyritään suojautumaan. Tällaisina uhkina mainitaan henkilötietojen vahingossa tai tahallisesti aiheutettu tuhoaminen, vahingossa aiheutettu häviäminen, laiton käsittely, luvaton luovuttaminen ja levittäminen sekä muuttaminen.

Artiklassa annetaan lisäksi komissiolle valta määritellä tarkemmin mitä edellä mainituilta tekniikkaan ja organisaatioon liittyviltä vaatimuksilta käytännössä milloinkin edellytetään antamalla delegoituja säädöksiä.[113] Tällaisilla delegoiduilla säädöksillä voidaan komission toimesta vahvistaa merkitys esimerkiksi sille, mitä *uusin tekniikka* käytännön tasolla kulloinkin tarkoittaa.

5.2 Tietoturva nykyisessä lainsäädännössä

Henkilötietolaissa tietoturvasta säädetään seitsemännessä luvussa. Lain 32 §:ssä säädetään, että rekisterinpitäjän on *toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä*. Lisäksi samassa pykälässä määrätään, että toimenpiteitä toteutettaessa huomioon on otettava *käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta*.

[113] 86 artiklan mukaisesti

Tietoturvaa voidaan tarkastella eri näkökulmista. Tietoturvaa voidaan ensinnäkin pitää yhtenä keskeisimmistä tietoturvasäädöksien yleisperiaatteista. Tällöin korkean tietoturvan vaatimus on itsestäänselvyys ja keskeinen periaate säädettäessä tietoturvasäädöksiä. Tietoturvan itsessään voidaan nykypäivänä katsoa kuuluvan yksilön perusoikeuksien joukkoon. Tietoturva voidaan nähdä ns. metaperusoikeutena, joka takaa osaltaan muiden perusoikeuksien toteutumisen. Voidaan ajatella, että riittävä tietoturvan taso on välttämätön edellytys henkilötietojen suojan toteutumiselle.[114]

Rekisterinpitäjän kannalta katsottuna kysymyksessä on puolestaan lähinnä velvollisuus huolehtia siitä, että tietoja ei luvattomasti käsitellä – kuten myös henkilötietolain 32 § asian ilmaisee. Toisaalta 32 §:n toinen momentti tuo keskeisesti mukaan myös suhteellisuusperiaatteen. Toisin sanoen tarkkaa turvallisuuden tasoa ei ole määritelty laissa, vaan taso on määriteltävä olosuhteiden mukaisesti määritettävän suojaamistarpeen mukaan. Tällainen lainsäädäntötapa tuo joustavuutta harkintaan, jota varjostaa jatkuvasti kehittyvä tietotekniikka ja siihen liittyvät tekniset sovellutukset. Samalla kuitenkin, kun tarkkoja tietoturvan vaatimustasoja ei ole määritelty, joudutaan käytännön tasolla harkitsemaan entistä tarkemmin milloin riittävä tietoturvan taso on saavutettu. Tällaiseen harkintaan vaikuttavat luonnollisesti myös – erityisesti rekisterinpitäjän kannalta katsottuna – taloudelliset seikat. On selvää, että mitä korkeammaksi tietoturvan taso asetetaan, niin sitä korkeammaksi nousevat myös järjestelyistä rekisterinpitäjälle aiheutuneet kustannukset. Vaikka lähtökohdaksi harkinnassa onkin syytä asettaa yksilön perusoikeus riittävän korkean tason omaavaan tietoturvaan, on syytä kiinnittää myös huomiota siihen, minkälaisia taloudellisia menoeriä kustakin tietoturvaa koskevasta ratkaisusta toimijoille aiheutuu. Saarenpää muistuttaakin osuvasti, että laissa ei ole pyritty absoluuttiseen tietoturvan tasoon.[115]

Tietoturvasta puhuttaessa keskeisenä näkökantana usein nähdään tietotekniikan turvallisuuteen liittyvä puoli. Onkin selvää, että ilman salattuja teknisiä tietoverkkoja ja muita tietoturvallisia teknisiä välineitä, ei voida toteuttaa vaadittavia tietoturvan tasoja. On kuitenkin syytä muistaa, että tietoturvaan kuuluu teknisen tietoturvallisuuden lisäksi myös muita aspekteja. Tällainen muu

[114] Saarenpää (2012), s. 320
[115] Saarenpää (2012), s. 336-337

seikka, joka vaikuttaa tietoturvan tasoon, on esimerkiksi henkilöstöturvallisuus. Organisaatiossa on syytä kiinnittää huomiota muiden muassa siihen miten tietoja käsittelevät henkilöt koulutetaan ottamaan huomioon tieturvaan liittyvät seikat. Myös se, kenellä itse organisaation sisällä on pääsy tietoihin, on määriteltävä: muilta kuin niiltä, jotka käsittelevät tietoja tehtäviensä hoitamiseksi, on estettävä pääsy tietoihin.[116]

Oikeudellisessa mielessä tietoturvan voidaan katsoa muodostuvan kolmesta eri tyyppisestä osa-alueesta, jotka turvaavat tietoa ja siihen liittyvää tietojenkäsittelyä sekä tietoliikenneinfrastruktuuria. Ensimmäinen näistä osa-alueista on *luottamuksellisuuden* turvaaminen. Tällöin keskeistä on varmistaa, että turvattaviin tietoihin sekä tietoihin liittyviin tietojenkäsittelytoimiin ja järjestelmiin on pääsy vain niillä, joilla siihen on oikeus. Tällöin tulee varmistaa, että turvattavia tietoja ei päädy oikeudetta ulkopuolisten haltuun. Toinen keskeinen seikka on *eheyden* vaatimus. Tämän vaatimuksen ajatuksena on tietoturvalle asetettu vaatimus siitä, että tiedot ja niihin liittyvät järjestelmät ja palvelut eivät vahingossa tai tahallisen toiminnan seurauksena pääse muuttumaan tai tuhoutumaan. Kolmas tietoturvan osa-alue on *käytettävyys*. Tällä puolestaan tarkoitetaan sitä, että tietojen ja niihin liittyvien järjestelmien tulee olla käytettävissä ilman häiriöitä ja viiveitä oikea aikaisesti. Voidaan katsoa, että oikeusjärjestyksen säädökset, jotka koskevat näitä kolmea osa-aluetta, muodostavat yhdessä oikeudellisessa mielessä tietoturvan käsitteen.[117]

Henkilötietolaissa määritelty tietoturva on kaikkea henkilötietojen käsittelyä koskeva yleinen määräys. Lainsäädännössä on lisäksi lukuisia erityisiä määritelmiä tietoturvalle. Tällaisina lainkohtina voidaan mainita Sähköisen viestinnän tietosuojalain 2 § 13 momentti sekä samaisen lain 19 § 1 momentti.[118] Lukuisista eri tietoturvalle annetuista määritelmistä johtuen, tietoturvan tasoa määritettäessä onkin syytä kiinnittää huomiota henkilötietolain lisäksi myös muussa lainsäädännössä annettuihin määritelmiin.[119]

Tietosuojavaltuutetun toimisto on julkaissut lukuisia ”tarkastuslistoja”, joiden avulla rekisterinpitäjät voivat itse tarkistaa onko omassa organisaatiossa

[116] Saarenpää (2012), s. 336-337
[117] Korhonen (2012), s. 438
[118] Saarenpää (2012), s. 372
[119] Saarenpää (2012), s. 337-338

huolehdittu riittävällä tavalla laissa edellytetyistä tietoturvan vaatimista seikoista. Tarkastuslistoissa kysytään esimerkiksi; onko työntekijöiden kanssa tehty salassapitosopimukset, onko varmistettu, että tietojen käsittelyssä käytetyt välineet ovat turvallisia sekä onko tiedot varmuuskopioitu ja miten varmuuskopioiden säilyttäminen on järjestetty. Tietosuojavaltuutettu muistuttaa myös, että henkilötietolaissa säädetyt suunnittelu- ja huolellisuusvaatimukset ulottuvat koskemaan myös tietoturvasta huolehtimista.[120]

Nykyaikana tietotekniikkaan liittyvät toiminnot on usein ulkoistettu varsinaisen organisaation ulkopuolisille toimijoille. Tietotekniikan asiantuntija Petteri Järvinen näkee asian siten, että toimintojen ulkoistamiseen liittyy periaatteessa aina tietoturvariskejä. Hän perustelee tätä sillä, että ulkoistamisen yhteydessä rekisterinpitäjän ulkoinen viestiliikenne lisääntyy, joka puolestaan jo itsessään aiheuttaa riskin tietoturvalle. Lisäksi hän muistuttaa, että ulkoistamisen yhteydessä suora määräämisvalta ja valvonta toiminnoista siirtyy toimeksiantajan tavoittamattomiin ja tämä puolestaan saattaa aiheuttaa tietoturvalle omat riskinsä.[121]

5.3 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Asetusehdotuksen 31 artiklassa velvoitetaan rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle *ilman aiheetonta viivytystä* ja jos mahdollista, niin 24 tunnin kuluessa henkilötietojen tietoturvaloukkauksen ilmitulosta. Artiklassa ei tarkemmin määritellä mitä ilmaisulla ”ilman aiheetonta viivytystä tarkoitetaan”. Tähän voitaneen soveltaa yleiskielestä johdettua tulkintaa; ilmoitus on tehtävä valvontaviranomaiselle niin pian kuin se käytännössä on mahdollista.[122] Eräänlaisena rajapyykkinä artiklassa mainitaan 24 tuntia siitä ajankohdasta, jolloin tietoturvaloukkaus on tullut itse rekisterinpitäjän tietoon. Tämä merkitsee sitä, että jos tietoa tietoturvaloukkauksesta ei toimiteta 24 tunnin kuluessa, on rekisterinpitäjä velvollinen antamaan valvontaviranomaiselle *perustellun selityksen.* Tässä yhteydessä ei kuitenkaan ole tarkemmin määritelty sitä, mitä *perustellulla*

[120] Tietosuojavaltuutetun toimisto. Tietosuojan ja tietoturvan ”tee se itse”-tarkastus. Osoitteessa: http://www.tietosuoja.fi
[121] Järvinen (2002), s. 114
[122] Valittava esimerkiksi nopein yhteydenottotapa useiden tapojen ollessa mahdollisia

selityksellä tarkemmin tarkoitetaan. Myös henkilötietojen käsittelijä on velvollinen ilmoittamaan henkilötietoja koskevasta tietoturvaloukkauksesta. Tällöin ilmoitus tehdään rekisterinpitäjälle ja se on tehtävä heti kun tietoturvaloukkaus on tullut tietoon.

Artiklan kolmannessa kohdassa määritellään valvontaviranomaiselle tehtävän ilmoituksen sisällölle asetetut minimivaatimukset:

a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien kyseessä olevien rekisteröityjen ryhmät ja lukumäärät sekä tietueiden ryhmät ja lukumäärät;

b) ilmoitettava tietosuojavastaavan henkilöllisyys ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

c) suositeltava toimenpiteitä, joilla lievennetään henkilötietojen tietoturvaloukkauksen mahdollisia haittavaikutuksia;

d) kuvattava henkilötietojen tietoturvaloukkauksen seurauksia;

e) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta.

Luetellut sisällölliset minimivaatimukset ovat jossain määrin tulkinnanvaraisia sillä ne ovat luonteeltaan ainakin joltain kohdin melko suuripiirteisiä. Varsinkin kohdat c, d ja e jättävät helposti avoimia kysymyksiä. Varsinkin se, miten tarkoin määritelmin - esimerkiksi tietoturvaloukkauksen seurausten kohdalla – kuvailua tulee ilmoituksessa suorittaa, jää helposti tulkinnanvaraiseksi kysymykseksi. Tämä lieneekin tarkoitushakuista sillä artiklassa siirretään valtaa komissiolle antamalla sille oikeus säätää delegoituja säädöksiä, joissa määritellään tarkemmin tämän artiklan ensimmäisen ja toisen kohdan soveltamisen kriteerit ja edellytykset.[123] Komissiolle siirretään myös valta antaa säädös vakiomuotoisesta ilmoituksesta, jolla edellä mainittu rekisterinpitäjän ilmoitusvelvoite voidaan täyttää.[124]

Edellä mainitun lisäksi rekisterinpitäjä velvoitetaan dokumentoimaan kaikki hänen organisaatiota koskevat tietoturvaloukkaukset. Näiden dokumenttien pohjalta valvontaviranomaisen on tarvittaessa pystyttävä tarkistamaan, että rekisterinpitäjälle asetettuja velvoitteita on noudatettu.

[123] 86 artiklan mukaisesti
[124] Täytäntöönpanosäädös 87 artiklan 2 kohdan tarkastusmenettely

5.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Kun 31 artikla koski henkilötietojen tietoturvaloukkauksen ilmoittamisvelvollisuudesta viranomaiselle, niin 32 artikla puolestaan koskee henkilötietojen tietoturvaloukkauksen ilmoittamisesta rekisteröidylle itselleen.

Artiklan ensimmäisessä kohdassa säädetään, että rekisterinpitäjän on tilanteissa, joissa tietoturvaloukkauksella on todennäköisesti haittavaikutuksia henkilötietojen suojalle tai rekisteröidyn yksityisyydelle, ilmoitettava tietoturvaloukkauksesta rekisteröidylle *ilman aiheetonta viivytystä.* ”Ilman aiheetonta viivytystä” voitaneen tässäkin tilanteessa tulkita samoin kuin edellä 31 artiklan kohdalla eli ts. yleiskielen mukaisessa merkityksessään. Tässä artiklassa tosin ei ole asetettu erityistä 24 tunnin erityisvelvoiteaikaa kuten 31 artiklassa.

Toinen tulkintaa ainakin jossain määrin edellyttävä seikka on se, miten korkealle on asetettava rima arvioidessa todennäköisyysastetta, kun arvioidaan tietoturvaloukkauksen mahdollisia haittavaikutuksia ja rekisteröidyn yksityisyydelle aiheutuvia vaikutuksia. Mielestäni kysymystä tulee katsoa rekisteröidyn oikeuksia painottavasta näkökulmasta ja tällöin todennäköisyysaste tuleekin asettaa suhteellisen matalalle. Artiklassa annetaan komissiolle valta säätää tarkempia säädöksiä, joissa määritellään kriteerit tietoturvaloukkauksia koskevien ilmoitusten arviointitilanteille.[125]

Artiklan toisessa kohdassa määritellään rekisteröidylle annettavan ilmoituksen sisältö. Ensinnäkin ilmoituksessa on kerrottava millainen tietoturvaloukkaus on ollut luonteeltaan. Lisäksi viitataan 31 artiklan kohtaan, jossa määritellään millainen viranomaiselle annettavan ilmoituksen sisältö on oltava. Rekisteröidylle annettavassa ilmoituksessa tosin edellytetään ainoastaan, että ilmoituksesta on käytävä ilmi tietosuojavastaava yhteystietoineen tai muu yhteydenottokanava, josta saa lisätietoja tarvittaessa. Lisäksi ilmoituksessa on suositeltava toimenpiteitä, joilla tietoturvaloukkauksen mahdollisia haittavaikutuksia voidaan mahdollisesti omin toimin minimoida. Edellä mainitut ovat vain ilmoituksen sisällölle asetetuttuja minimivaatimuksia, joten tämän

[125] 86 artiklan mukaisesti

lisäksi rekisteröidylle voitaneen antaa ilmoituksessa muutakin tietoturvaloukkaukseen liittyvää relevanttia informaatiota.

Artiklan kolmannessa kohdassa säädetään tilanteesta, jossa tietoturvaloukkaus on tapahtunut, mutta rekisterinpitäjällä on ollut käytössä tekninen välineistö, joka on taannut sen, että vääriin käsiin joutuneiden henkilötietojen sisältö on ollut sellaisessa muodossa, että niitä ei ole ulkopuolinen taho pystynyt tulkitsemaan. Rekisterinpitäjällä on velvollisuus osoittaa kyseisten teknisten välineiden toimivuus valvontaviranomaiselle. Kun edellä mainitut edellytykset ovat täyttyneet, niin tietoturvaloukkauksesta ei tarvitse ilmoittaa rekisteröidylle.

Valvontaviranomainen voi vaatia rekisterinpitäjää tekemään ilmoituksen tietoturvaloukkauksesta rekisteröidylle, jos rekisterinpitäjä ei tätä oma-aloitteisesti ole tehnyt. Ennen rekisterinpitäjälle tehtävää vaatimusta valvontaviranomainen arvioi millaisia todennäköisiä haittavaikutuksia tietoturvaloukkauksella on saattanut olla.

5.5 Tietoturvaloukkauksista ilmoittaminen nykyisin

Itse henkilötietolaissa ei nykyisin säädetä yleisestä kaikkia rekisterinpitäjiä koskevasta velvollisuudesta ilmoittaa henkilötietojen tietoturvaloukkauksista viranomaiselle tai edes rekisteröidylle itselleen. Sen sijaan sähköisen viestinnän tietosuojalaissa ilmoitusvelvollisuudesta säädetään. Sähköisen viestinnän tietosuojalaki koskee sähköisten viestintäpalvelujen tarjoajia. Lisäksi elokuussa 2013 tuli voimaan sähköisen viestinnän palveluntarjoajien ilmoitusvelvollisuuksia täsmentävä ja yhtenäistävä asetus: Euroopan komission asetus N:o 611/2013. Asetuksen tarkoituksena on yhtenäistää unionin tasolla varsin erilaisia käytäntöjä, koskien sähköisen viestinnän tietosuojadirektiivissä säädettyjä ilmoitusvelvollisuuksia.

Tietoturvaloukkauksia koskevia ilmoituksia täsmentävässä asetuksessa säädetään sähköisen viestinnän palveluntarjoajalle velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksesta kansalliselle viranomaiselle 24 tunnin sisällä siitä ajankohdasta, jona loukkaus havaittiin. Ilmoituksessa on oltava tiedot tietoturvaloukkauksen luonteesta siinä laajuudessa, kun ilmoitusvaiheessa tiedetään, tieto tietoturvaloukkauksen kohteeksi joutuneiden henkilötietojen luonteesta ja sisällöstä sekä lisäksi tiedot toimista, joihin

palveluntarjoaja tietoturvaloukkauksen johdosta on ryhtynyt tai aikoo ryhtyä. Myös tieto mahdollisista muista palveluntarjoajista, joita tietoturvaloukkaus koskee, on liitettävä mukaan tietosuojaviranomaiselle annettavaan ilmoitukseen. Ensimmäistä tietoturvaloukkauksesta annettavaa ilmoitusta luonnehditaan asetuksessa alustavaksi ilmoitukseksi. Kun tietoturvaloukkauksen luonne ja sisältö tarkentuu, on palveluntarjoajan annettava täydentävä tietoturvaloukkausta koskeva ilmoitus viranomaiselle mahdollisimman pian – kuitenkin viimeistään kolmen päivän kuluttua alustavasta ilmoituksesta.[126]

Viestintävirasto, joka toimii Suomessa kansallisena viranomaisena, jolle tietoturvaloukkausta koskeva ilmoitus annetaan, kehottaa omassa ohjeistuksessaan palveluntarjoajia tekemään ensimmäisen ilmoituksen nopeaa yhteysvälinettä käyttäen, esimerkiksi puhelimitse. Myöhempi täydentävä ilmoitus suositetaan annettavaksi kirjallisessa muodossa. Mikäli tietoturvaloukkaus kestää pidemmän aikajakson ajan kehotetaan palveluntarjoajaa pitämään Viestintävirasto ajan tasalla tilanteen kehityksestä.[127]

Ilmoitusvelvollisuuksia tarkentavassa asetuksessa säädetään lisäksi sähköisen viestinnän palveluntarjoajaa koskevasta ilmoitusvelvollisuudesta palvelun tilaajille ja käyttäjille. Tällöin ilmoitusvelvollisuus on sidottu arvioon siitä, onko tietoturvaloukkauksella *todennäköisiä* haittavaikutuksia tilaajan tai käyttäjän henkilötiedoille tai yksityisyydelle. Harkinnan tueksi asetuksessa on lueteltu seikkoja, jotka tällöin erityisesti tulee ottaa huomioon. Tällaisia harkinnassa erityisesti huomioon otettavia seikkoja ovat tietoturvaloukkauksessa mukana olleiden henkilötietojen luonne ja sisältö, tietoturvaloukkauksen yleiseen luonteeseen liittyvät olosuhteet sekä lisäksi arviot siitä, millaisia seurauksia tietoturvaloukkauksella todennäköisesti on tietoturvaloukkauksen kohteeksi joutuneille tilaajille tai henkilöille.[128]

---

[126] Väkeväinen Heidi: Palveluntarjoajan velvollisuus ilmoittaa tietoturvaloukkauksesta täsmentyy. www.merilampi.com

[127] Viestintävirasto. Tietoturvaloukkausilmoitus.
Osoitteessa: https://www.viestintavirasto.fi

[128] Väkeväinen Heidi: Palveluntarjoajan velvollisuus ilmoittaa tietoturvaloukkauksesta täsmentyy. www.merilampi.com

Tilaajille ja käyttäjille annettavan ilmoituksen sisällöstä on myös määräykset asetuksessa. Tietoturvaloukkauksen kohteelle annettavassa ilmoituksessa on palveluntarjoajan nimen lisäksi oltava tieto muiden muassa ajankohdasta, jolloin tietoturvaloukkaus on todennäköisesti tapahtunut, tieto siitä mitä seurauksia tietoturvaloukkauksesta sen kohteeksi joutuneelle todennäköisesti aiheutuu sekä lisäksi myös tieto siitä mihin toimenpiteisiin palveluntarjoaja on tietoturvaloukkauksen takia ryhtynyt. On syytä muistaa, että ilmoitusvelvollisuus koskee niitä palveluntarjoajia, jotka ovat suoraan sopimussuhteessa tilaajaan tai henkilöön, joka on tietoturvaloukkauksen kohteena. Tilanteesta, jossa palveluntarjoaja käyttää alihankkijan palveluksia, säädetään asetuksen 5 artiklassa. Tällöin alihankkija on velvollinen tekemään välittömästi ilmoituksen tietoturvaloukkauksesta sitä alihankkijana käyttävälle palveluntarjoajalle.[129]

6 TIETOSUOJAA KOSKEVA VAIKUTUSTENARVIOINTI JA ENNAKKOHYVÄKSYNTÄ

6.1 Tietosuojaa koskeva vaikutustenarviointi

Asetusehdotuksen 33 artiklan ensimmäisessä kohdassa säädetään, että jos tietojenkäsittelyssä käsitellään materiaalia johon liittyy niiden *luonteen, laajuuden tai tarkoitusten vuoksi rekisteröidyn oikeuksien ja vapauksien kannalta erityisiä riskejä,* on rekisterinpitäjän tällöin tehtävä arvio vaikutuksista joita käsittelystä aiheutuu henkilötietojen suojalle.

Artiklan toisessa kohdassa luetellaan tilanteet, joihin erityisesti tulee soveltaa arvion laatimisvelvoitetta. Tällaisia ns. korkean riskin tilanteita ovat tämän mukaisesti esimerkiksi a.) tilanteet, joissa käsitellään automatisoidulla menetelmällä henkilön taloudelliseen tilanteeseen, terveyteen tai mieltymyksiin liittyviä tietoja b.) tilanteet, joissa keräämällä tietoa yksilöiden terveydestä, rodusta tai etnisestä alkuperästä, tehdään yksilöitä tai suurempia joukkoja koskevia päätöksiä c.) yleisten tilojen videovalvonta d.) biometristen ja geneettisten tietojen käsittely suuressa mittakaavassa e.) toimet, joissa viranomainen katsoo, että on suoritettava ennakkokuuleminen[130]. Mielestäni luetteloa tulee pitää ainoastaan esimerkkiluettelona, sillä artiklan sanamuodosta

[129] Väkeväinen Heidi: Palveluntarjoajan velvollisuus ilmoittaa tietoturvaloukkauksesta täsmentyy. www.merilampi.com

[130] 34 artiklan 2b-kohdan mukaisesti

voi arvioida, että myös muunlaisetkin tilanteet – tilanteet, jotka eivät sisälly luetteloon - voivat tulla arvioiduksi ns. korkean riskin tilanteina.

Artiklan kolmannessa kohdassa määritellään vaikutuksia koskevan arvioinnin sisältö. Sisällölle säädetään minimivaatimukset. Ensinnäkin mukana on oltava yleinen esittely niistä tietojenkäsittelytoimista, joita aiotaan toteuttaa. Lisäksi on oltava arvio niistä riskeistä, joita saattaa aiheutua käsittelytoimista rekisteröidyn oikeuksille ja vapauksille sekä toimista, joilla näiltä riskeiltä suojaudutaan. Tämän lisäksi arvioinnissa on pystyttävä osoittamaan keinot, joilla varmistetaan henkilötietojen suojan toteutuminen sekä se, että tämän asetusehdotuksen säädöksiä noudatetaan. Myös sen, että kaikkien osapuolten oikeuksia noudatetaan tietojenkäsittelyssä, on käytävä ilmi arvioinnista. Komissiolle on artiklassa annettu oikeus antaa arvioinnin sisältöä koskevia tarkentavia säädöksiä. Artiklan neljännessä kohdassa määrätään lisäksi, että rekisterinpitäjän on tiedusteltava rekisteröityjen mielipiteitä suunnitelluista käsittelytoimista.

Artiklassa säädetään myös poikkeuksesta edellä mainittuun. Jos kysymyksessä on julkishallinnon orgaani, joka käsittelee henkilötietoja lakisääteisen velvoitteen toteuttamiseksi, ei tämän artiklan säädöksiä pääsääntöisesti sovelleta. Lisäksi komissiolle annetaan valta säätää tarkempia säädöksiä koskien sitä, miten määritellään ne tilanteet, joihin liittyy erityisiä riskejä.[131]

6.2 Arkaluonteiset henkilötiedot ja niiden käsittely nykyisin

Kaikkea henkilötietojen käsittelyä, niiden luonteesta riippumatta, koskee henkilötietolain 6 §, joka edellyttää henkilötietojen käsittelyyn liittyvää suunnittelua. Suunnitteluvelvoite koskee koko henkilötiedon elinkaarta - aina tiedon keräämisestä sen hävittämiseen saakka.[132] Henkilötietolaissa ei ole asetusehdotuksen 33 artiklan mukaista säännöstä velvollisuudesta laatia erityistä vaikutusarviointia määrätynlaisten henkilötietojen käsittelyjen yhteydessä. Sen sijaan henkilötietolain 3 luvussa säädetään arkaluonteisten henkilötietojen ja henkilötunnuksen erityisasemasta. Asetusehdotuksen 33 artiklaa voidaankin pitää ainakin jossain määrin rinnasteisena henkilötietolain 3.

[131] 86 artiklan mukaisesti
[132] Alapuranen (2012), s. 74

lukuun, sillä säädetäänhän siinä erityisesti sellaisten henkilötietojen käsittelystä, jotka omaavat arkaluonteisuuden takia erityisen tietosuojariskin.

Henkilötietojen käsittelylle pitää olla aina lain mukainen peruste. Laissa arkaluonteisiksi määriteltyjen henkilötietojen kohdalla käsittely on vieläkin rajoitetumpaa, sillä henkilötietolain 11 §:n lähtökohtana on arkaluonteisten henkilötietojen käsittelykielto.[133] Arkaluonteisiin henkilötietoihin luetaan kuuluviksi esimerkiksi terveyteen liittyvät tiedot, tieto ammattiliittoon kuulumisesta, sekä rotua tai etnistä alkuperää koskevat tiedot. Lain 12 §:ssä säädetään poikkeusperusteista, joiden nojalla arkaluonteisia henkilötietoja voidaan käsitellä. Pääasiallisena poikkeusperusteena toimii yksilön itsensä antama lupa arkaluonteisten henkilötietojen käsittelylle. Muita poikkeusperusteita, joiden vallitessa käsittely on sallittua, ovat esimerkiksi rekisteröidyn tai muun henkilön elintärkeän edun suojaaminen, lakiin perustuva oikeutus sekä tietosuojalautakunnan antama erityislupa, joka sallii käsittelyn. Arkaluonteiset henkilötiedot tulee poistaa henkilörekisteristä heti kun lainmukaista perustetta niiden käsittelylle ei enää ole. Tarvetta käsittelylle tulee arvioida aina kuitenkin vähintään viiden vuoden välein.[134]

Henkilötietolain 13 §:ssä säädetään puolestaan henkilötunnuksen erityisasemasta. Henkilötunnuksen käsittely on sallittua rekisteröidyn yksiselitteisesti antamalla suostumuksella. Henkilötunnuksen käsittely on lisäksi sallittua, jos käsittelystä säädetään laissa tai jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää, esimerkiksi rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamisen takia. Käsittely sallitaan myös tilanteissa, joissa harjoitetaan luotonantoa, saatavien perintää taikka vuokraustoimintaa. Henkilötunnusta käsiteltäessä rekisterinpitäjän tulee huolehtia siitä, että henkilötunnusta ei kuitenkaan *merkitä tarpeettomasti henkilörekisterin perusteella tulostettuihin tai laadittuihin asiakirjoihin*.[135]

6.3 Ennakkohyväksyntä ja ennakkokuuleminen

Asetusehdotuksen 34 artiklassa säädetään tilanteista, joissa henkilötietojen käsittelyn laillisuuden edellytyksenä on viranomaisen ennakkohyväksyntä

[133] Vanto (2011), s. 44
[134] Ollila (2002), s. 308-309
[135] Salminen (2009), s. 75-76

toiminnalle tai viranomaisen suorittama ennakkokuuleminen. Rekisterinpitäjän tai henkilötietojen käsittelijän on kahdessa eri tyyppisessä tilanteessa saatava viranomaisen ennakollinen hyväksyntä suunnittelemalleen henkilötietojen käsittelylle.

Ensinnäkin hyväksyntä on saatava tilanteissa, jossa rekisterinpitäjä tai henkilötietojen käsittelijä käyttää toiminnassaan asetusehdotuksen 42 artiklan 2 d-kohdan mukaisia sopimuslausekkeita. Artiklassa 42 säädetään henkilötietojen siirroista ns. kolmansiin maihin ja kansainvälisille järjestöille. Alakohta 2 d koskee erityisesti tilanteita, joissa tietojen siirto oikeutetaan viranomaisten ennakkohyväksymien sopimuslausekkeiden perusteilla. Toisin sanoen 2 d-alakohdassa tarkoitetaan nimenomaan tätä 34 artiklan mukaista ennakkohyväksymisprosessia.

Toinen tilanne, jossa viranomaisen ennakkohyväksyntää edellytetään, on käsillä silloin, kun rekisterinpitäjä tai henkilötietojen käsittelijä aikoo siirtää henkilötietoja kolmansiin maihin tai kansainvälisille järjestöille, mutta samanaikaisesti se ei kuitenkaan takaa henkilötietojen suojaa sellaisella metodilla, joka olisi oikeudellisesti sitova. Tällä viitataan asetusehdotuksen 42 artiklan 5 alakohtaan: *rekisterinpitäjän tai henkilötietojen käsittelijän on saatava ennakkohyväksyntä siirrolle tai siirtojen sarjalle tai säännöksille, jotka sisällytetään tällaisen siirron perusteet muodostaviin hallinnollisiin järjestelyihin*.

Ennakkokuulemisvelvoitteesta säädetään artiklan toisessa kohdassa. Rekisterinpitäjän tai henkilötietojen käsittelijän on määrätyissä tilanteissa kuultava viranomaista ennen henkilötietojen käsittelyn aloittamista. Ennakkokuulemisen tarkoituksena on varmistaa, että tämän asetusehdotuksen säännöksiä tullaan noudattamaan sekä rekisteröidylle mahdollisesti aiheutuvat riskit pystytään minimoimaan kaavaillussa henkilötietojen käsittelyssä.

Ennakkokuulemisvelvoite on ensinnäkin silloin, kun asetusehdotuksen 33. artiklan vaikuttavuusarviointi viittaa siihen, että käsillä olevaan henkilötietojen käsittelyyn liittyy *todennäköisesti* erityisiä riskejä. Artiklan sanamuoto viittaa siihen, että varmuutta riskeistä ei tarvita, vaan pelkkä todennäköisyysaste on riittävä peruste ennakkokuulemiselle. Lisäksi artiklassa on annettu komissiolle

valtaa säätää tarkempia säädöksiä koskien erityisten riskien määrittämiskriteerejä.[136]

Toinen tilanne, jossa viranomaisen ennakkokuulemista tulee soveltaa, on käsillä silloin, kun perusteena on sellainen toimenpide, joka kuuluu viranomaisen ennakolta laatimaan luetteloon. Artiklan mukaisesti valvontaviranomaisen tulee ennakollisesti laatia ja julkistaa lista sellaisista henkilötietojenkäsittelytoimista, joihin liittyy rekisteröidyn kannalta katsottuna erityisiä riskejä oikeuksiin ja vapauksiin liittyen. Jos suunnitellun henkilötietojen käsittelyn katsotaan kuuluvan luonteeltaan listalla julkaistujen toimien joukkoon, tulee ennakkokuulemisvelvoite täyttää.

Valvontaviranomaisen tullessa - ennakkohyväksymiskäsittelyn tai ennakkokuulemiskäsittelyn jälkeen - siihen lopputulokseen, että kaavailtu henkilötietojen käsittely ei tule täyttämään tämän asetusehdotuksen asettamia edellytyksiä, tulee sen kieltää henkilötietojen käsittely sekä antaa tarvittavat ehdotukset toimista, joilla puutteet voidaan korjata.

6.4 Tietosuojavaltuutetulle tehtävät ilmoitukset

Tietosuojavaltuutetulle tehtävistä ilmoituksista säädetään henkilötietolain 8. luvussa. Ilmoitusten avulla tietosuojavaltuutettu valvoo ennakolta henkilötietojen lainmukaisen käsittelyn toteutumista. On syytä muistaa, että ilmoituksen jättäminen ei kuitenkaan ole henkilötietojen käsittelyn lainmukaisuutta juridisesti vahvistava menettely; toisin sanoen kysymys ei ole ennakkohyväksymisprosessista. Tietosuojavaltuutetun julkaisemassa oppaassa tietosuojavaltuutetulle tehtävät ilmoitusvelvollisuudet on nimetty niiden luonteen mukaan: *rekisteri-ilmoitus, toimintailmoitus* sekä *ilmoitus henkilötietojen luovuttamisesta ulkomaille*.[137]

Lähtökohtana henkilötietolaissa on, että henkilötietojen automaattisesta käsittelystä on tehtävä ilmoitus tietosuojavaltuutetulle. Ilmoitus tehdään toimittamalla rekisteriseloste tietosuojavaltuutetulle. On syytä huomata, että henkilötietolain 36 §:ssä tarkoitetaan nimenomaan automaattisen tietojenkäsittelyn avulla suoritettua henkilötietojen käsittelyä, joten manuaalinen

[136] 86 artiklan mukaisesti
[137] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 3

henkilötietojen käsittely jää tämän velvoitteen ulkopuolelle. Käytännössä kuitenkin suurin osa myös automaattisesta henkilötietojen käsittelystä jää velvoitteen ulkopuolelle, sillä samaisessa pykälässä säädetään lukuisista poikkeuksista, jolloin ilmoitusvelvollisuutta ei ole. Voidaan katsoa, että silloin kun henkilörekisteriä käsitellään osittain automaation keinoin ja osin manuaalisesti on tällöin ilmoitukseen sisällytettävä tiedot kokonaisuudessaan eli tiedot kumminkin tavoin käsitellyistä rekisterin osista ilman, että manuaalisesti käsitellyt osat jätettäisiin pois. Myös se, että henkilörekisterin tiedot sijaitsevat fyysisesti eri paikoissa, ei vaikuta ilmoitusvelvollisuuden laajuuteen, vaan koko käyttötehtävän perusteella muodostuvaa loogista rekisteriä käsitellään yhtenä kokonaisuutena myös ilmoitusvelvollisuuden osalta.[138]

Kuten aiemmin mainittiin, suuri osa automaattisen tietojenkäsittelyn tilanteista rajataan 36 §:n 4 momentin mukaan pois ilmoitusvelvollisuudesta. Tällaisia tilanteita, joissa ilmoitusta tietosuojavaltuutetulle ei tarvitse tehdä ovat esimerkiksi tilanteet; joissa henkilötietoja käsitellään rekisteröidyn yksiselitteisen suostumuksen perusteella, tilanteet joissa asiakkaita tai työntekijöitä koskevia henkilötietoja käsitellään konsernin sisällä sekä tilanteet, joissa henkilötietoja käsitellään laissa annetun valtuutuksen pohjalta. Lisäksi samaisessa momentissa säädetään, että asetus tason säädöksillä voidaan säätää myös muista poikkeuksista, jolloin ilmoitusta ei tarvitse antaa. Tällaisen asetuksilla säätämisen edellytyksenä kuitenkin on, että tällöin on *ilmeistä* että henkilötietojen käsittelyllä ei loukata yksilön *yksityisyyden suojaa taikka hänen oikeuksiaan tai vapauksiaan*. Aina ei kuitenkaan rekisterinpitäjille käytännön tasolla ole selvää, kuuluvatko he siihen piiriin, joiden ei tarvitse antaa ilmoitusta tietosuojavaltuutetulle. Tietosuojavaltuutetun toimistosta muistutetaankin rekisterinpitäjille suunnatussa ohjeistuksessa, että epäselvissä tilanteissa on parempi antaa ilmoitus kuin jättää se antamatta.[139]

Henkilötietolain 36 §:n toisen momentin ensimmäisessä kohdassa säädetään ilmoitusvelvollisuudesta määrätyissä sellaisissa tilanteissa, joissa henkilötietoja siirretään ulkomaille. Tämän mukaisesti rekisterinpitäjä on velvoitettu määrätyissä tilanteissa, joissa henkilötietoja siirretään Euroopan unionin ulkopuolelle, tekemään ilmoituksen siirroista tietosuojavaltuutetulle. Kun

[138] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 3-4
[139] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 7

momentissa säädetyt edellytykset täyttyvät, koskee ilmoitusvelvollisuus kaikkia henkilötietojen luovutuksia, mukaan luettuna myös tilanteet, joissa kysymyksessä on toimeksiannon toteuttamisen takia tehtävät henkilötietojen siirrot sekä konsernin sisällä toteutettavat henkilötietojen siirrot. Tällaiseen ilmoitukseen, joka koskee henkilötietojen siirtämistä ulkomaille, tulee liittää rekisteriselosteen lisäksi tieto siitä minkä tyyppistä tietoa siirretään sekä tieto siitä, miten tietojen siirtäminen käytännössä toteutetaan.[140]

Myös määrätyntyyppiset toimialat on katsottu henkilötietolaissa sellaisiksi, että niissä käsitellään yleensä suuria määriä henkilötietoja, joten yksilön edun mukaista on, että tällaisten toimialan toimijoilla on ilmoitusvelvollisuus toiminnastaan. Henkilötietolain 36 § 3 momentissa säädetäänkin toimialoista, joita elinkeinona tai toisen lukuun harjoitettaessa on tehtävä ns. toiminta-ilmoitus. Lain kohdan mukaan muiden muassa perintätoimintaa sekä luottotietotoimintaa elinkeinona harjoittavat ovat ilmoitusvelvollisia toiminnastaan. Myös tahot, jotka harjoittavat toisen lukuun ns. työntekijöiden soveltuvuustestausta ja valintaa sekä toimijat, jotka toisen lukuun harjoittavat tietojenkäsittelytehtäviä, ovat velvoitettuja tekemään ilmoituksen toiminnastaan tietosuojavaltuutetulle. Toimintailmoitus annetaan harjoitettavasta toiminnasta yleensä, joten sitä ei tarvitse antaa erikseen jokaisesta laissa säädetystä alaan kuuluvasta suoritetusta toimesta.[141]

Ns. automatisoitujen päätöksentekojärjestelmien käyttöönotosta on myös säädetty ilmoitusvelvollisuus. Henkilötietolain 36 §:n 2 momentin 2 kohdassa viitataan automatisoidulla päätöksentekojärjestelmällä samaisen lain 31 §:ssä määriteltyyn automatisoituun päätökseen, jossa arvioidaan rekisteröidyn määrättyjä ominaisuuksia ja joka tehdään pelkästään automatisoidun tietojenkäsittelyn perusteella. Tällaisen järjestelmän käyttöönotosta on tehtävä ilmoitus tietosuojavaltuutetulle. Ilmoituksesta tulee rekisteriselosteen lisäksi käydä ilmi millaiseen logiikan pohjalta automaattinen järjestelmä päätöksen tekee.[142] Tällaisia automaattisia päätöksentekojärjestelmiä käyttävät esimerkiksi ns. pikalainayhtiöt.

[140] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 10
[141] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 8-10
[142] Tietosuojavaltuutetun toimisto. Henkilötietolain mukainen ilmoitusvelvollisuus, s. 8

7 TIETOSUOJAVASTAAVA

7.1 Tietosuojavastaavan nimittäminen

Asetusehdotuksen 35 artiklassa määritellään tietosuojavastaavan nimittämiseen liittyvät edellytykset ja itse tietosuojan henkilöön liittyvät seikat. Rekisterinpitäjän ja henkilötietojen käsittelijän on aina nimitettävä tietosuojavastaava ensinnäkin niissä tapauksissa, kun tietojenkäsittely tapahtuu julkihallinnon elimen tai viranomaisen toimesta. Toinen vastaava tilanne, jossa tietosuojavastaavan nimittämistä edellytetään aina, on silloin kun tietojenkäsittelijänä on yritys, jonka palveluksessa on vähintään 250 työntekijää. Kolmas tällainen tilanne on käsillä silloin, kun rekisterinpitäjän tai henkilötietojen käsittelijän *keskeiset tehtävät* ovat sellaisia, että ne *luonteensa, laajuutensa ja/tai tarkoitustensa vuoksi edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa.* Muissa kuin edellä mainituissa tilanteissa tietosuojavastaavaan nimittäminen on vapaaehtoista.

Artiklan viidennessä kohdassa määritellään tietosuojavastaavan pätevyyteen liittyvät seikat. Tietosuojavastaavaa valittaessa on otettava erityisesti huomioon ehdokkaiden ammattipätevyys; huomioiden erityisesti tietosuojalainsäädäntöä koskeva tietämys. Lisäksi luonnollisesti on otettava huomioon se, että henkilöllä on valmiudet suoriutua keskeisistä 37 artiklassa määritellyistä tietosuojavastaavan tehtävistä. Voidaan kysyä kuinka korkealle ammattipätevyyden ja tietämyksen taso tulee asettaa valintaprosessia suoritettaessa. Artiklassa annetaan eräänlainen yleisluonteinen määritelmä, jonka mukaan tietosuojavastaavan valintaprosessissa tulee vaatimustaso asettaa sen mukaan minkätyyppistä tietojenkäsittelyä rekisterinpitäjän tai tietojenkäsittelijän toimesta harjoitetaan sekä sen mukaan kuinka korkeaa tietosuojan tasoa käsiteltävät tiedot edellyttävät. Komissiolle on tässäkin tilanteessa siirretty valta antaa tarkentavia säädöksiä[143], joissa määritellään tarkemmat yksityiskohdat tietosuojavastaavan pätevyyden määrittämiselle.

Tietosuojavastaavan toimintaa järjestettäessä on lisäksi varmistettava, että eturistiriitoja ei pääsisi aiheutumaan, kun päätetään tietosuojavastaavan muista kuin tietosuojavastaavan tehtäviin liittyvistä työtehtävistä organisaatiossa. Tietosuojavastaava voi toimia suoraan rekisterinpitäjän tai henkilötietojen

[143] 86 artiklan mukaisesti

käsittelijän alaisuudessa tai vaihtoehtoisesti hän voi hoitaa tehtäviään varsinaisen organisaation ulkopuolelta toimeksiantosopimuksen pohjalta.

Lisäksi artiklassa esitetään, että tietosuojavastaava on valittava aina vähintään kahden vuoden ajaksi. Hänet voidaan erottaa tehtävästään vain, jos hän ei enää täytä tehtävälle asetettuja pätevyysvaatimuksia. Tietosuojavastaavan nimi ja yhteystiedot on annettava valvontaviranomaiselle sekä yleisölle. Keskeinen merkitys rekisteröidyn kannalta on se, että rekisteröity voi milloin tahansa ottaa yhteyden tietosuojavastaavaan häneen itseensä liittyvissä tietojenkäsittelyä koskevissa asioissa sekä lisäksi vaatia samalla tämän asetuksen hänelle suomien oikeuksien täyttämistä.

7.2 Tietosuojavastaavan asema

Artiklassa 36 määritellään tarkemmin tietosuojavastaavan asema osana organisaatiota. Rekisterinpitäjän tai henkilötietojen käsittelijän on ensinnäkin otettava *asianmukaisesti ja riittävän ajoissa* tietosuojavastaava mukaan kaikkiin toimiin, joissa käsitellään henkilötietojen suojaan liittyviä kysymyksiä. Sillä, mitä asianmukaisuuden käsitteellä tässä yhteydessä tarkoitetaan, ei ole tarkemmin artiklassa määritelty. Mielestäni tässä yhteydessä asianmukaisuudelle tulee asettaa perusteeksi tavoite, että toimitaan tämän asetuksen hengen mukaisessa mielessä ja asetuksen tavoitteiden toteuttamista edistävin toimin. Se, milloin *riittävän ajoissa* määritelmä toteutuu, taas lienee paljolti kiinni itse toteutettavan toimen luonteesta.

Toiseksi, rekisterinpitäjän tai henkilötietojen käsittelijän on turvattava sellaiset toimintapuitteet, joissa tietosuojavastaava voi toimia riippumattomasti. Riippumattomuuteen kuuluu myös se, että tietosuojavastaavan asema järjestetään sellaiseksi, että siihen liittyvien tehtävien hoitamiseen ei pyritä vaikuttamaan ulkopuolisin ohjein. Lisäksi säädetään, että tietosuojavastaava raportoi havainnoistaan ja tehtäviinsä liittyvistä seikoista suoraan organisaation johdolle.

Myös se, että tietosuojavastaava käytännön tasolla pystyy toteuttamaan 37 artiklassa hänelle määrätyt velvoitteensa, on rekisterinpitäjän tai henkilötietojen käsittelijän vastuulla. Käytännössä tämä tarkoittaa sitä, että tietosuojavastaavalle on annettava riittävät resurssit harjoittaa toimiaan. Näihin

kuuluvat esimerkiksi toimitilojen ja henkilöstön järjestäminen tietosuojavastaavan käyttöön.

7.3 Tietosuojavastaavan tehtävät

Artikla 37 puolestaan määrittelee tietosuojavastaavan tehtävien sisällön. Tässä artiklassa nimenomaan määritellään minimisisältö tietosuojavastaavan tehtäväkentälle. Käytännössä tietosuojavastaavan tehtäviin voi kuulua myös muita henkilötietojen suojaan liittyviä tehtäviä kuin vain tässä artiklassa säädettyjä.

Tietosuojavastaavan on ensinnäkin informoitava rekisterinpitäjää sekä henkilötietojen käsittelijää tämän asetuksen heille asettamista velvoitteista. Tähän liittyen tietosuojavastaava laatii dokumentit annetuista tiedoista ja saaduista vastauksista. Toinen keskeinen tietosuojavastaavan tehtävä on seurata henkilötietojen suojaan liittyvien toimenpiteiden käytännön täytäntöönpanoa. Näihin tehtäviin kuuluu esimerkiksi seurata miten henkilötietojen käsittelyyn liittyvät henkilöt koulutetaan tehtäviinsä sekä se kuinka henkilötietojen käsittelyyn liittyvät organisaation sisäiset tarkastukset suoritetaan.

Lisäksi tietosuojavastaava velvoitetaan *seuraamaan* sitä, miten tämän asetuksen säännöksiä toteutetaan henkilötietojen käsittelyssä. Se, mitä *seuraamisella* käytännön tasolla tarkoitetaan, on jätetty avoimeksi. Syynä tähän lienee se, että artiklassa on annettu komissiolle valta säätää tarkempia säädöksiä siitä, miten artiklassa tietosuojavastaavalle annettuja velvoitteita käytännössä tulkitaan ja sovelletaan. Artiklan asettamien vaatimusten toteutumisen yleisen seuraamisen lisäksi tietosuojavastaavan tehtäviin kuuluu artiklan mukaisesti erityisesti vastuu seurata *sisäänrakennettuun tietosuojaan, oletusarvoiseen tietosuojaan ja tietoturvallisuuteen* liittyvien seikkojen toteutumista. Edellä mainittujen lisäksi tietosuojavastaavan tehtäväksi määrätään myös velvollisuus seurata rekisteröidylle ilmoittamiseen liittyviä toimintoja sekä rekisteröidyiltä tulevien pyyntöjen käsittelyä.

Tietosuojavastaavan vastuulla on myös huolehtia siitä, että asetusehdotuksen 28. artiklassa määritellyt asiakirjat säilytetään. Artiklassa 28 asetetaan rekisterinpitäjälle ja hänen edustajilleen velvoite säilyttää henkilötietojen

käsittelystä syntyneet asiakirjat. Näiden yleisten henkilötietojen käsittelyyn liittyvien asiakirjojen säilyttämisvelvoitteesta huolehtimisen lisäksi tietosuojavastaava velvoitetaan *seuraamaan* tietosuoturvaloukkauksiin liittyvien asiakirjojen säilyttämistä sekä tietoturvaloukkauksiin liittyvän ilmoitusvelvollisuuden toteutumista[144].

Tietosuojavastaava velvoitetaan lisäksi *seuraamaan* tietosuojaa käsittelevän vaikutusarvioinnin laatimista. Myös *ennakkohyväksyntään* ja *ennakkokuulemiseen* liittyvien prosessien seuraaminen ovat tietosuojavastaavan tehtäväkentässä. Myös yhteydenpito valvontaviranomaisen suuntaan on tietosuojavastaavan tehtävänä. Tietosuojavastaavan tulee toimia yhteyshenkilönä valvontaviranomaisen suuntaan tietojenkäsittelyyn liittyvissä asioissa. Hänen tulee ensinnäkin seurata sitä, miten valvontaviranomaisen esittämiin pyyntöihin vastataan. Lisäksi tietosuojavastaavalla on eräänlainen yleisvelvoite toimia yhteistyössä valvontaviranomaisen kanssa silloin kun valvontaviranomainen sitä pyytää. Yhteistyö voi toisaalta tapahtua myös tietosuojavastaavan omasta aloitteesta.

7.4 Tietosuojavastaavan asema nykyisessä lainsäädännössä

Henkilötietolaissa ei nykyisin säädetä tietosuojavastaavasta. Näin ollen yleistä rekisterinpitäjän velvollisuutta nimetä tietosuojavastaava ei Suomessa nykyisin ole. Sen sijaan erityislaissa on edellytetty määrättyjen rekisterinpitäjien nimeävän tietosuojavastaava organisaatioonsa. Määräys tietosuojavastaavan nimittämisvelvollisuudesta sisältyy lakiin sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä lakiin sähköisestä lääkemääräyksestä. Erityislainsäädäntö velvoittaa esimerkiksi Kansaneläkelaitoksen sekä kaikkien apteekkien nimeämään tietosuojavastaavan.[145]

Tietosuojavaltuutettu on antanut ohjeistuksen koskien tietosuojavastaavaa ja hänen tehtäviään. Ohjeistuksessa tietosuojavastaavan keskeiseksi tehtäväksi nähdään auttaminen siinä, että rekisterinpitäjä pystyy toteuttamaan sille lainsäädännössä asetetut velvoitteet koskien henkilötietojen lainmukaista käsittelyä. Näihin rekisterinpitäjälle kuuluviin velvoitteisiin, joiden toteutumisen

[144] Velvollisuudet määritelty artikloissa 31 ja 32
[145] Vanto (2011), s. 184

varmistamisessa tietosuojavastaava on mukana, kuuluu velvollisuus laatia tietosuojaseloste, velvollisuus määritellä tietojen keräämisen ja käsittelyn tarkoitus sekä velvollisuus huolehtia käsiteltävien henkilötietojen suojaamisesta. Ohjeistuksessa kuitenkin painotetaan sitä faktaa, että vaikka tietosuojavastaava osallistuukin keskeisesti tietojenkäsittelyyn liittyvien velvoitteiden toteuttamiseen, niin tämä ei kuitenkaan poista rekisterinpitäjälle kuuluvaa viimesijaista oikeudellista vastuuta huolehtia kyseisistä velvoitteista.[146]

On syytä muistaa, että henkilötietojen käsittelyä voi tapahtua periaatteessa organisaation kaikilla osa-alueilla aina tuotannosta operatiiviseen johtoon asti, joten myös tietosuojavastaavan tehtäväkentän tulee yhtälailla olla tarpeeksi laaja ja kaikki osa-alueet kattava.[147] Tietosuojavaltuutetun antamassa ohjeistuksessa hahmotellaan tietosuojavastaavalle kuuluvien työtehtävien toimenkuvaa. Tietosuojavastaavan tulee toimia erityisasiantuntijana, joka avustaa asiantuntemuksellaan niin organisaation henkilökuntaa kuin johtoporrasta. Tietosuojavastaavan toiminnan tulee edistää hyvän henkilötietojen käsittelytavan toteutumista. Ohjeistukseen on luetteloitu tehtäviä, joiden katsotaan kuuluvan tietosuojavastaavalle. Tietosuojavastaava toimii yhdyslinkkinä viranomaisten ja organisaation välillä henkilötietojen käsittelyyn liittyvissä asioissa. Lisäksi hän osallistuu suunnittelutoimintaan, joka koskee henkilötietojen käsittelyyn liittyvien asioiden järjestämistä organisaatiossa. Tietosuojavastaavan tehtäviin kuuluu valvoa kaikkea organisaatiossa tapahtuvaa henkilötietojen käsittelyä ja tarvittaessa saattaa huomaamansa epäkohdat organisaation johdon tietoisuuteen.[148]

Tietosuojavastaavan toiminta tulisi järjestää organisatorisesti siten, että hän pystyisi toimimaan mahdollisimman itsenäisesti, jotta hänelle määriteltyjen tehtävien tarkoitukset toteutuisivat mahdollisimman tehokkaasti. Tietosuojavastaavan koulutustasolle ei ole asetettu erityisiä vaatimuksia. Tietosuojavaltuutetun ohjeistuksessa kuitenkin huomautetaan, että tietosuojavastaavalla tulisi olla sellainen koulutus, jolla hän selviää hänelle määrätyistä tehtävistä. Tietosuojavastaavana voi toimia myös organisaation ulkopuolinen taho, sillä sitä ei ole lainsäädännössä erityisesti kielletty. Tällöin

[146] Tietosuojavaltuutetun toimisto. Tietosuojavastaavan toimenkuva, tehtävät ja asema, s. 2
[147] Salminen (2009), s. 26
[148] Tietosuojavaltuutetun toimisto. Tietosuojavastaavan toimenkuva, tehtävät ja asema, s.2-3

voidaan katsoa, että organisaatio voi ulkoistaa tietosuojavastaavan tehtävät ulkopuolisen toimijan hoidettavaksi.[149] Vanto kuitenkin muistuttaa, että tietosuojavastaavana ei voi toimia osakeyhtiö, vaan tietosuojavastaavan on aina oltava luonnollinen henkilö.[150]

8 KÄYTÄNNESÄÄNNÖT JA SERTIFIOINTI

8.1 Käytännesäännöt

Artiklassa 38 säädetään käytännesäännöistä. Käytännesäännöillä tarkoitetaan ohjeistuksia siitä, miten eri aloilla toimivien yritysten, yhteisöjen ja viranomaisten tulisi toiminnassaan ottaa huomioon henkilötietojen käsittelyyn liittyviä seikkoja. Näillä ohjeistuksilla ja suosituksilla pyritään turvaamaan erityisesti yksilön yksityisyyttä turvaavien perusoikeuksien toteutuminen.[151]

Artiklan ensimmäinen kohta antaa eräänlaisen yleisluonteisen julistuksen, jolla velvoitetaan valvontaviranomaiset sekä jäsenvaltiot, mutta myös itse komissio edistämään omilla toimillaan sellaisten käytännesääntöjen laatimista, jotka tukevat luonteeltaan tämän asetusehdotuksen säännösten toteutumista. Tähän yhteyteen on liitetty myös luettelo, jossa luetellaan seikat, jotka tulisi erityisesti ottaa huomioon. Tällaisia toiminnassa huomioon otettavia seikkoja ovat muiden muassa läpinäkyvyydenperiaatteen huomioon ottaminen, henkilötietojen keräämiseen liittyvät seikat, henkilötietojen siirtäminen ns. kolmansiin maihin sekä menetelmät, joilla varmistetaan, että rekisterinpitäjät noudattavat heitä koskevia käytännesääntöjä.

Jäsenvaltioiden tasolla valvontaviranomaisille annetaan oikeus antaa lausuntoja siitä, ovatko ehdotetut käytännesäännöt sisällöltään tämän asetuksen mukaisia. Itse unionin tasolla vastaavanlainen oikeus annetaan komissiolle silloin, kun kysymyksessä ovat käytännesäännöt, jotka pyritään saattamaan voimaan unionin laajuisesti. Tällöin komissio voi antaa täytäntöönpanosäädöksiä, joissa se toteaa, että määrätyt käytännesäännöt ovat päteviä koko unionin laajuisesti.[152]

---

[149] Tietosuojavaltuutetun toimisto. Tietosuojavastaavan toimenkuva, tehtävät ja asema, s. 3
[150] Vanto (2011), s. 188
[151] Toimialakohtaisten käytännesääntöjen laatiminen. Tietosuojavaltuutetun toimisto, www.tietosuoja.fi
[152] 87 artiklan mukaisesti

8.2 Käytännesäännöistä henkilötietolaissa

Käytännesääntöjen keskeisimpänä tavoitteena voidaan nähdä halu edistää, eri alojen erityispiirteet huomioon ottaen, kansallisten säädösten moitteetonta käytännön soveltamista.[153] Toimialakohtaisista käytännesäännöistä säädetään henkilötietolain 42 §:ssä. Pykälän mukaisesti rekisterinpitäjät tai niitä edustavat järjestöt voivat laatia käytännesääntöjä henkilötietolain soveltamiseksi sekä ”hyvän tietojenkäsittelytavan edistämiseksi”. Hyvä tietojenkäsittelytapa on mainittu jo henkilötietolain 1 §:ssä lain tavoitteena. Hyvä tietojenkäsittelytapa on abstrakti käsite ja sitä ei ole sen tarkemmin itse pykälässä määritelty. Hyvä tietojenkäsittelytapa voidaan nähdä eräänlaisena optimointikäskynä lain soveltajalle; lain eri säännöksiä on tulkittava siten, että sen tavoitteiden mukainen yksilön yksityisyys ja muut perusoikeudet toteutuvat.[154]

Käytännesäännöt voidaan toimittaa tietosuojavaltuutetun arvioitavaksi. Tietosuojavaltuutetulle on säädetty oikeus tarkistaa käytännesääntöjen lainmukaisuus. Käytännössä, jos käytännesäännöt täyttävät lain mukaiset edellytykset, tietosuojavaltuutettu arvioituaan käytännesäännöt toteaa ne asianmukaisiksi. Jos lainmukaisuus ei tietosuojavaltuutetun mielestä toteudu, niin yleensä käytännesääntöjen laatijaa kehotetaan muokkaamaan tai täydentämään käytännesääntöjä.[155]

On syytä muistaa, että tietosuojavaltuutettu tarkistaessaan käytännesäännöt, ei varsinaisesti oikeudellisessa mielessä vahvista käytännesääntöjä sitoviksi, vaan kysymyksessä on niiden lainmukaisuuteen kohdistuva arvioimistoimi. Tällöin tietosuojavaltuutetulle ei muodostu viranomaisvastuuta eikä asianmukaisuuden toteaminen myöskään siirrä vastuuta käytännesääntöjen oikeellisuudesta niille rekisterinpitäjiä edustaville yhteisöille, jotka ovat laatineet käytännesäännöt. Sen sijaan tietosuojavaltuutetun asianmukaisiksi toteamille käytännesäännöille voidaan antaa käytännön toiminnassa olettama, että niitä noudattamalla tietojenkäsittelyssä noudatetaan lakia.[156] Toimialakohtaisia käytännesääntöjä on laadittu esimerkiksi sukututkimusta sekä telemarkkinointia varten.[157]

[153] Salminen (2009), s. 47
[154] Saarenpää (2012), s. 338
[155] Vanto (2011), s. 171
[156] Saarenpää (2012), s. 342
[157] Vanto (2011), s. 171

Tietosuojalainsäädäntöä voidaan pitää vaikeasti hahmotettava lainsäädännön alueena. Tietosuojalainsäädännön säädökset ovat usein hyvin abstrakteja, joka osaltaan vaikuttanee siihen, että varsinkin juridiikkaa tuntemattoman on usein vaikea tulkita normien todellisia merkityssisältöjä. Tästä johtunee ainakin jossain määrin se, että tietosuojan alueelta käytännesääntöjä on laadittu runsaasti. Toisena syynä tietosuojaa käsitteleville käytännesäännöille erityisesti Suomen kohdalla on varmasti myös se, että lainsäädäntömme ei tunne muualla Euroopassa yleisesti käytettyä paikallisen tason tietosuojaviranomaista. Edellä jo mainittujen lisäksi on syytä myös muistaa, että itse tietosuojavaltuutetun aktiivisuus käytännesääntöjen käyttämistä tukevana alullepanijana, on varmasti myös osaltaan vaikuttanut käytännesääntöjen suosioon.[158] Yhtenä tällaisena edistävänä toimena voidaan nähdä tietosuojavaltuutetun julkaisema ohjeistus käytännesäännöistä.[159]

Tietosuojavaltuutetun käytännesääntöjä koskevassa ohjeistuksessa muistutetaan, että käytännesäännöissä pystytään ottamaan huomioon erityisesti kunkin toimialan toimintaan liittyvät erityispiirteet. Lisäksi muistutetaan mahdollisuudesta kääntyä tietosuojavastaavan puoleen jo käytännesääntöjen laatimisvaiheessa, jolloin tietosuojavastaava voi resurssiensa sallimissa rajoissa antaa asiantuntevaa neuvontaansa ja ohjausta jo tässä vaiheessa. Myös itse käytännesääntöjen rakenteeseen liittyviä ehdotuksia on sisällytetty ohjeistukseen. Lopuksi myös huomautetaan, että käytännesäännöistä tulisi käydä ilmi myös se, mihin lainsäädäntöön käytännesääntöjen ohjeet loppujen lopuksi pohjautuvat eli useimmiten käytännössä henkilötietolakiin.[160]

8.3 Sertifiointi

Asetusehdotuksen artikla 39 velvoittaa komission ja jäsenvaltiot *edistämään* sellaisten sertifiointimenetelmien käyttöönottoa, joiden avulla rekisteröidyt voivat vaivattomasti arvioida rekisterinpitäjien tietosuojan tasoa. Artiklassa ei tarkemmin määritellä sertifiointimenetelmien yksityiskohtia. Niiden tulee kuitenkin luonteeltaan olla sellaisia, että ne edistävät tämän asetuksen päämääriä. Komissiolle annetaan valta säätää tarkempia normeja koskien

[158] Saarenpää (2012), s. 341-342
[159] Tietosuojavaltuutetun toimisto. Toimialakohtaisten käytännesääntöjen laatiminen.
[160] Vanto (2011), s. 171-172

sertifikaattien sisältöä ja luonnetta sekä mekanismeja, joiden vallitessa sertifikaatti voidaan kulloinkin myöntää.[161]

8.4 Tietoturvasertifikaateista nykyisen lainsäädännön valossa

Viestintäviraston tehtäviin kuuluu valvoa tietoturvallisuutta arvioivien arviointilaitosten toimintaa. Yritykset voivat arviointilaitoksen suorittaman arvioinnin avulla osoittaa esimerkiksi yhteistoimintakumppaneilleen organisaationsa korkean tietoturvallisuuden tason. Tietoturvallisuuden tason osoittaminen voi olla joskus jopa pakollista. Tällainen tilanne voi yritykselle tulla vastaan esimerkiksi silloin, kun se tarjoaa palvelujaan julkisyhteisön toimijalle.[162] Vaikka organisaation toimintaa ei olisi edes tarkoitus virallisesti sertifioida, voidaan tietoturvasertifioinnin malleja noudattamalla saattaa organisaation tietoturvakäytännöt kätevästi turvalliselle tasolle[163].[164]

Laissa tietoturvallisuuden arviointilaitoksista (22.12.2011/1405) säädetään menettelystä, jossa Viestintävirasto antaa hyväksyntänsä arviointilaitoksen toiminnalle. Laissa määritellään arviointilaitosten hyväksytyksi tulemiselle asetetut edellytykset. Näitä edellytyksiä ovat, että arviointilaitos on riippumaton arvioinnin kohteesta, arviointilaitoksella on toiminnan edellyttämät laitteet ja välineistöt sekä lisäksi arviointilaitoksen työntekijöillä tulee olla riittävä koulutus ja kokemus. Tietoturvallisuuden arviointilaitosten tulee tuntea niihin sovellettava lainsäädäntö ja muut niitä koskevat ohjeet ja määräykset. Jos myöhemmin havaitaan, että aiemmin Viestintäviraston hyväksymä arviointilaitos ei enää täytäkään hyväksymiselle asetettuja vaatimuksia, voidaan hyväksyminen Viestintäviraston toimesta perua. Lain 9 §:ssä säädetään lisäksi arviointilaitosten tehtävistä. Arviointilaitosten tehtäviin kuuluu toimeksiantonsa mukaisesti tarkistaa arvioinnin kohteen toimitilat ja järjestelmät ja arvioida sitä, täyttyvätkö tietoturvallisuudelle asetetut vaatimustasot.[165]

Määrätyissä tilanteissa tietojenkäsittelyjärjestelmiltä edellytetään viranomaistasoista hyväksyntää. Kun lain mukaisesti hyväksytty arviointilaitos suorittaa arvioinnin, jossa todetaan, että järjestelmä täyttää sille edellytetyt

[161] 86 ja 87 artiklojen mukaisesti
[162] Tietoturvallisuuden arviointilaitokset. Viestintävirasto, www.viestintavirasto.fi
[163] Yleisimmin käytetty tietoturvallisuuden standardi ISO 27001
[164] Lagus (2013), s. 13
[165] Viestintävirasto. Ohje tietoturvallisuuden arviointilaitoksille, s. 5, 8-9

tietoturvallisuuden kriteerit, voidaan viranomaishyväksyntä tehdä tämän arvioinnin perusteella. Vaikka arviointilaitoksen arviointia voidaankin käyttää lähtökohtana tietoturvallisuutta arvioidessa, tekee lopullisen päätöksen järjestelmän tietoturvallisuuskriteerien täyttymisestä aina nimenomaan toimivaltainen turvallisuusviranomainen. Hyväksyessään järjestelmän tietoturvallisuuskriteerien mukaiseksi, antaa viranomainen päätöksestä todistuksen.[166]

9 EUROOPAN PARLAMENTIN OIKEUDELLISTEN ASIOIDEN VALIOKUNNAN LAUSUNTO

Euroopan parlamentin Oikeudellisten asioiden valiokunta (JURI) julkaisi yleistä tietosuoja-asetusta koskevan oman lausuntonsa 25.3.2013.[167] Vaikka lausunnossa todetaankin, että valiokunta on tyytyväinen komission työhön, niin ehdottaa valiokunta lukuisia muutoksia komission asetusesitykseen.[168] Rekisterinpitäjän kannalta katsottuna keskeisiä muutosehdotuksia ovat erityisesti artikloita 25, 33, 36 ja 39 koskevat muutosehdotukset. Seuraavaan olen ottanut tarkempaan esittelyyn muutaman näistä muutosehdotuksista.

Asetusehdotuksen 25 artiklassa säädetään unionin ulkopuolelle sijoittautuneen rekisterinpitäjän velvollisuudesta asettaa edustaja unionin alueella tapahtuvaa toimintaansa varten. Artiklassa on säädetty myös poikkeuksista, jolloin edustajaa ei kuitenkaan tarvitse asettaa. Valiokunta ehdottaa muutosta 25 artiklan 2b-kohtaan, jossa säädetään, että yrityksellä jolla on alle 250 työntekijää, ei tarvitse edustajaa toiminnalleen asettaa. Valiokunnan mielestä tilanteissa, joissa rekisterinpitäjäyrityksellä on alle 250 työntekijää, tulisi valvontaviranomaiselle antaa valta päättää siitä, onko tarpeellista asettaa edustaja unionin alueella tapahtuvalle toiminnalle. Tällöin edustajan asettamisvelvoitteen kriteerinä pidettäisiin käsiteltävien tietojen erityistä riskialttiutta tai asianosaisten suurta määrää.[169]

---

[166] Viestintävirasto. Ohje tietoturvallisuuden arviointilaitoksille, s. 33

[167] Euroopan parlamentin Oikeudellisten asioiden valiokunta (JURI): Lausunto oikeudellisten asioiden valiokunnalta kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus), annettu 25. maaliskuuta 2013.

[168] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 3

[169] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 59-60

Asetusehdotuksen 33 artiklassa säädetään tietosuojaa koskevasta vaikutusarvioinnista. Oikeudellisten asioiden valiokunta ehdottaa ensinnäkin artiklan toisen kohdan sanamuotoon muutosta. Artiklan toinen kohta voidaan sanamuodoltaan tulkita siten, että lueteltujen käsittelytoimien luettelo on yleisluonteinen eli kysymykseen voi tulla myös luettelossa mainitsematon henkilötietojen käsittelyä koskeva toimi. Valiokunta katsoo, että oikeusturvan kannalta toisen kohdan sanamuotoa tulisi muuttaa siten, että luetteloa pidettäisiin kattavana, jolloin luetteloon kuulumattomia käsittelytoimia tämän artiklan määräykset eivät koskisi. Valiokunta ehdottaa lisäksi, että artiklan neljäs kohta tulisi poistaa kokonaan. Neljännessä kohdassa säädetään rekisterinpitäjän velvollisuudesta määrätyissä tilanteissa kysyä rekisteröityjen tai heidän edustajiensa mielipiteitä suunnitelluista henkilötietojen käsittelytoimista. Artiklan neljännen kohdan poistamista valiokunta perustelee kohtuuttomuusnäkökannalla. Valiokunnan mielestä olisi suhteettoman kova vaatimus vaatia kaikkia rekisterinpitäjiä toimialasta riippumatta tiedustelemaan rekisteröityjen mielipiteitä suunnitelluista käsittelytoimista.[170]

Artiklan 33 viidettä kohtaa esitetään oikeudellisten asioiden valiokunnan lausunnossa myös muutettavaksi. Viidennessä kohdassa rajataan julkishallinnon elimet pääsääntöisesti vaikutusarviointivelvoitteen ulkopuolelle. Tällaista, rekisterinpitäjän oikeudelliseen luonteeseen perustuvaa rajausta, valiokunta ei pidä hyvänä ratkaisuna, vaan rajaus tulisi artiklassa määritellä siten, että se perustuisi siihen, minkälaista palvelua luonteeltaan tarjottava palvelu on. Tätä palvelun luonteeseen perustuvaa rajaustapaa valiokunta pitää parempana siitä syystä, että julkishallinnon tehtäviä annetaan usein yksityisten organisaatioiden tehtäväksi. Myös artiklan kuudes kohta, jossa annetaan komissiolle valta säätää tarkentavia säädöksiä koskien 33 artiklaa, tulisi valiokunnan mielestä poistaa kokonaisuudessaan. Tätä perustellaan sillä, että antamalla komissiolle delegoitujen säädösten säätämisvalta tämän artiklan osalta, annettaisiin komissiolle tällöin valta säätää *asetuksen kannalta olennaisista seikoista*. Valiokunta katsoo, että tällaisista *olennaisista seikoista* tulisi säätää itse asetuksessa. Valiokunta ei tosin perusteluissaan sen

[170] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 66-68

tarkemmin argumentoi mitä se tarkoittaa määritelmällä *asetuksen kannalta olennaiset seikat*.[171]

Asetusehdotuksen 36 artiklassa säädetään tietosuojavastaavan asemasta osana organisaatiota. Oikeudellisten asioiden valiokunta katsoo, että artiklan sanamuodossa painotetaan liialti sitä olettamaa, että tietosuojavastaavat olisivat lähtökohtaisesti työ- tai virkasuhteessa rekisterinpitäjään. Valiokunnan mielestä huomioon tulisi ottaa paremmin myös tilanteet, joissa tietosuojavastaavan tehtävät on sopimusperusteella ulkoistettu organisaation ulkopuoliselle taholle. Tästä johtuen 36 artiklan virke *Rekisterinpitäjän tai henkilötietojen käsittelijän on tuettava tietosuojavastaavaa tämän tehtävien suorittamisessa ja annettava tälle henkilöstö, toimitilat, varusteet ja muut resurssit* jne. tulisi valiokunnan mielestä muuttaa tarveharkintaiseen muotoon; *Rekisterinpitäjän tai henkilötietojen käsittelijän on tuettava tietosuojavastaavaa tämän tehtävien suorittamisessa ja tarvittaessa annettava tälle henkilöstö, toimitilat, varusteet ja muut resurssit* jne.[172]

Asetusehdotuksen 39 artiklaa, joka koskee tietosuojaa koskevia sertifiointeja ja niiden käytön edistämistä, valiokunta haluaisi muuttaa erityisesti siten, että artiklassa kovin avoimeksi jätetyt toimet sertifiointimenetelmien kehittämiseksi ja käyttöönottamiseksi määriteltäisiin huomattavasti yksityiskohtaisemmin. Asetusehdotuksessa käytetty termi *sertifiointimekanismit* on muutettu valiokunnan lausunnossa muotoon *sertifiointipolitiikat*. Ilmeisesti syynä tälle sanavalinnalle on se, että valiokunta on halunnut painottaa sitä, että sen mielestä komission tehtävä on hyväksyä käytetyt sertifiointimenetelmät. Lisäksi sertifiointipolitiikat tulisi ennen komissiossa hyväksymistä suunnitella ja valmistella Euroopan tietosuojaneuvostossa. Valiokunta painottaa myös, että sertifiointipolitiikoissa tulisi ottaa huomioon asianomaisten toimijoiden toimialojen erityispiirteet. Erityisesti huomiota tulisi kiinnittää Pk-yritysten toimintaympäristöihin ja tarpeisiin. Huomiota olisi myös kiinnitettävä siihen, että sertifioinnista aiheutuvat kustannukset eivät nousisi asianomaisten toimijoiden kannalta katsottuna liian korkeiksi. Valiokunnan mukaan toimintamenetelmiin tulisi luoda säännökset siitä, miten vanhentuneet sertifioinnit uudistetaan ja saatetaan ajan tasalle. Tällöin myös tilanteeseen, jossa vakavia laiminlyöntejä

[171] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 66-68
[172] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 73

on tapahtunut, pitäisi pystyä puuttumaan nopeasti ja myönnetyt sertifikaatit pitäisi tällöin pystyä peruuttamaan välittömästi.[173]

10 TIETOSUOJATYÖRYHMÄN LAUSUNTO

Tietosuojatyöryhmä antoi maaliskuussa 2012 oman lausuntonsa koskien unionin tietosuojauudistusta.[174] Tietosuojatyöryhmä on tietosuojadirektiivin nojalla perustettu riippumaton asiantuntijoista koostuva neuvoa antava asiantuntijaelin, joka toimii tietosuojaan liittyvien kysymysten osa-alueella. Työryhmään kuuluu jäsenvaltioiden tietosuojaviranomaisten edustajia. Se antaa tietosuojaan liittyvistä kysymyksistä lausuntoja ja suosituksia komissiolle.[175]

Tietosuojatyöryhmä katsoo, että ehdotetun asetuksen aiempaa täsmällisemmillä säännöksillä on lainsäädäntöä selkiyttävä ja yhtenäistävä vaikutus unionin alueella. Tämän voidaan osaltaan vaikuttavan myös tietojen vapaampaan liikkuvuuteen unionin sisällä.[176] Tietosuojatyöryhmä pitää myönteisenä, että rekisteröityjen asemaa pyritään vahvistamaan säännöksillä, joilla lisätään rekisterinpitäjien vastuuta. Erityisen myönteisinä tietosuojauudistuksen säännöksinä tietosuojatyöryhmä pitää niitä säännöksiä, joissa rekisterinpitäjiä kannustetaan investoimaan menetelmiin, joilla saavutetaan korkea tietosuojan taso. Tällaisiksi säännöksiksi voidaan katsoa muiden muassa asetusehdotuksen 23 artikla[177] sekä 33 artikla[178]. Tietosuojatyöryhmä näkee myös sen positiivisena seikkana, että asetusehdotukseen on otettu yhtenäinen laajasti eri toimialoja koskeva tietoturvaloukkauksia koskeva ilmoitusvelvollisuus.

Lukuisista uusista oikeasuuntaisista säännöksistä huolimatta tietosuojatyöryhmä katsoo, että tietosuojauudistus kaipaa vielä monien säännöksien osalta tarkennuksia ja parannuksia. Seuraavassa on

[173] Euroopan parlamentin Oikeudellisten asioiden valiokunnan lausunto 25. maaliskuuta 2013, s. 74-75
[174] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista (00530/12/FI WP 191), annettu 23. maaliskuuta 2012.
[175] Tietosuojavaltuutetun toimisto. Tietosuojatyöryhmä.
Osoitteessa: http://www.tietosuoja.fi/14891.htm
[176] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 6
[177] Sisäänrakennettu tietosuoja ja oletusarvoinen tietosuoja
[178] Tietosuojaa koskeva vaikutusarviointi

rekisterinpitäjän kannalta katsottuna otettu käsittelyyn keskeisimmät tietosuojatyöryhmän muutosehdotukset.[179]

Tietosuojatyöryhmä näkee ongelmallisena komissiolle asetusehdotuksessa annetun oikeuden antaa delegoituja säädöksiä ja täytäntöönpanosäädöksiä.[180] Tietosuojatyöryhmä tosin myöntää, että määrättyjen säännösten soveltamisen kannalta tarvitaan tarkentavia säädöksiä sekä täytäntöönpanosäädöksiä. Tästä huolimatta valittu menetelmä, jossa komissiolle annetaan valta säätää perusoikeuksia koskevista seikoista delegoiduilla säädöksillä ja täytäntöönpanosäädöksillä, nähdään virheelliseksi valinnaksi. Tietosuojatyöryhmä pelkää, että delegoitujen säädösten ja täytäntöönpanosäädösten antaminen – niiden oletettavan runsaasta määrästä johtuen – saattaa kestää monia vuosia. Tämä puolestaan nähdään oikeusvarmuutta huojuttavana epäkohtana, erityisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden kannalta katsottuna. Tietosuojatyöryhmä ehdottaa, että epävarmuutta pystyttäisiin torjumaan siten, että komissio ennakolta ilmoittaisi mitä delegoituja säädöksiä ja täytäntöönpanosäädöksiä se tulee tulevaisuudessa antamaan sekä arviot ajankohdista jolloin kyseisiä säädöksiä tullaan antamaan.[181]

Tietosuojatyöryhmä ottaa lausunnossaan kantaa myös komission asetusehdotuksessa tekemään valintaan, jolla pienet ja keskisuuret yritykset (pk-yritykset) vapautetaan määrätyissä artikloissa sellaisista velvoitteista, jotka toisaalta taas ovat voimassa suurten yritysten kohdalla. Tällaisina artikloina, joihin on lisätty pk-yrityksiä koskevia rajoitteita, on lausunnossa nostettu esille 25 artikla[182], 28 artikla[183] sekä 35 artikla[184]. Tietosuojatyöryhmä huomauttaa myös, että lisäksi muutamiin artikloihin on komissiolle jätetty valta säätää delegoituja säädöksiä ja täytäntöönpanosäädöksiä lisätoimista pk-yritysten hyväksi. Tällaisina artikloina, joihin on jätetty komissiolle tällainen mahdollisuus, mainitaan esimerkiksi artikla 22[185] sekä artikla 33[186].[187]

---

[179] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 4
[180] 86 ja 87 artikloiden mukaisesti
[181] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 7
[182] Rekisterinpitäjän velvollisuus nimittää edustaja unionin alueelle
[183] Henkilötietojen käsittelyä koskevat asiakirjat
[184] Tietosuojavastaavan asettamisvelvoite
[185] Rekisterinpitäjän vastuu
[186] Tietosuojaa koskeva vaikutusarviointi

Tietosuojatyöryhmä katsoo, että asetusehdotuksessa valitut lakitekniset valinnat, joilla pk-yrityksille on säädetty tai voidaan myöhemmin säätää poikkeuksia rekisterinpidosta, ovat epätarkoituksenmukaisia ottaen huomioon sen, että rekisteröidylle tulisi taata samantasoiset oikeudet tietosuojaan riippumatta siitä, minkä suuruinen yksikkö tietoja käsittelee. Tietosuojatyöryhmä näkee erityisesti riskin siinä, että rekisterinpitoa koskevat poikkeusvaraukset saattavat johtaa henkilötietojen suojan kannalta *epäyhtenäisyyteen* ja *ei-toivottuihin tuloksiin*. Tietosuojatyöryhmä ei tosin lausunnossaan sen selvemmin tarkenna minkälaisia ei-toivottuja tuloksia se pelkää.[188]

Toisaalta tietosuojatyöryhmä myöntää myös sen, että jos kaikkia asetusehdotuksen velvoitteita sovellettaisiin myös pk-yrityksiin, saattaisivat velvoitteet muodostua niille liian suureksi rasitteeksi. Ratkaisuna tähän tietosuojatyöryhmä ehdottaakin, että sen sijaan että otetaan huomioon tietojen käsittelijän kokoluokka, huomioitaisiinkin tietojenkäsittelyn *luonne* ja *laajuus*. Poikkeuksia velvoitteista säädettäessä huomiota tulisi kiinnittää siihen, minkälaisia tietoja käsitellään sen sijaan, että valintakriteeriksi asetetaan se minkä suuruinen yksikkö niitä käsittelee.[189]

Tietosuojatyöryhmä pitää myönteisenä seikkana, että asetusehdotukseen on otettu 23 artikla, jossa säädetään sisäänrakennetusta tietosuojasta ja oletusarvoisesta tietosuojasta. Tosin se katsoo, että asetusehdotusta voisi joiltain osin vielä kehittää, jotta sisäänrakennetun tietosuojan ja oletusarvoisen tietosuojan tavoitteet toteutuisivat parhaalla mahdollisella tavalla. Tällaisina toimina tietosuojatyöryhmä ehdottaa muiden muassa, että palveluihin ja tavaroihin sisältyvät yksityisyyttä edistävät ominaisuudet olisi aktivoitava automaattisesti. Tällaisina palveluun sisältyvinä yksityisyyttä tukevina ominaisuuksina voitaneen esimerkiksi pitää sosiaalisen median sovelluksiin sisältyviä käyttäjien yksityisyyttä suojaavia perusasetuksia. Tämän lisäksi tietosuojatyöryhmä huomauttaa, että 23 artiklan mukaisesti komissiolle ehdotetaan oikeutta vahvistaa teknisiä standardeja tälle alalle. Tällä tietosuojatyöryhmä haluaa painottaa näkemystään siitä, että komission tulisi

[187] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 8
[188] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 8
[189] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 8

standardeja säätäessään kuulla Euroopan tietosuojaneuvostoa ja kansainvälisiä standardisointijärjestöjä.[190]

Tietosuojatyöryhmä ehdottaa, että asetusehdotukseen tulisi lisätä yleinen velvollisuus muuttaa käsiteltävät tiedot tunnistamattomaan muotoon silloin kun se olisi käytännössä mahdollista ja oikeasuhteista. Tällä tarkoitetaan käytännössä sitä, että salanimen käytön velvoite[191] ja tietojen anonymisointi tulisi sisällyttää esimerkiksi 23 artiklaan. Vaikka tietosuojatyöryhmä ei sen tarkemmin tarkenna käsitystään siitä, millaisissa tilanteissa tällaisiin toimiin olisi ryhdyttävä, katsoo se, että näillä menetelmillä voitaisiin parantaa tietosuojan tasoa.[192]

Tietosuojatyöryhmä ottaa kantaa myös asetusehdotukseen sisällytettyihin viranomaisia koskeviin poikkeuksiin. Tietosuojatyöryhmä huomauttaa, että tietosuojauudistuksen yhtenä tavoitteena on juuri lainsäädännön kattavuuden varmistaminen. Lausunnossa pidetään epäkohtana sitä, että lukuisissa asetusehdotuksen artikloissa julkiselle sektorille on annettu erityisasema. Asetusehdotuksessa on yleiseen etuun vedoten säädetty lukuisia poikkeuksia viranomaisten velvollisuuksiin rekisterinpidossa. Tietosuojatyöryhmän mielestä monet poikkeuksista ovat perusteettomia ja epätäsmällisesti määriteltyjä.[193]

Yhtenä esimerkkinä, julkisen sektorin rekisterinpitoa koskevista poikkeuksista, mainitaan asetusehdotuksen 33 artiklan 5 kohta: määrätyissä tilanteissa, kun rekisterinpitäjä on viranomainen tai julkishallinnon elin ja henkilötietojen käsittely perustuu laissa säädettyyn velvoitteeseen, ei samaisessa artiklassa määriteltyä tietosuojaa koskevaa vaikutusarviointia tarvitse suorittaa. Tietosuojatyöryhmä pitää 33 artiklan 5 kohtaa epäkohtana ja se katsookin, että ainoa perusteltu tilanne, jossa tietosuojan vaikutusarvioinnin tekemisvelvoitteesta voisi vapautua, olisi tapaus, jossa vaikutusarviointi on suoritettu jo lainsäätämisvaiheessa. Tietosuojatyöryhmä painottaa voimakkaasti näkökantaansa siitä, että asetusehdotukseen sisältyville julkista sektoria koskeville yleisluonteisille poikkeuksille ei ole perusteita. Se ehdottaakin, että julkista sektoria koskevat yleiset erivapaudet jätettäisiin pois ja sekä julkiseen että yksityiseen sektoriin

[190] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 11
[191] Pseudonymisointi
[192] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 11
[193] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 12-13

sovellettaisiin samoja säännöksiä niin pitkälti kuin se käytännössä on mahdollista.[194]

Myös asetusehdotuksen 25 artiklaa tietosuojatyöryhmä ehdottaa muutamilta kohdin muutettavaksi. Asetusehdotuksen 25 artiklassa säädetään Euroopan unionin ulkopuolelle sijoittautuneen rekisterinpitäjän velvollisuudesta asettaa edustaja unionin aluetta varten. Lausunnossa kritisoidaan sitä, että asetusehdotuksesta ei käy selvästi ilmi millainen asema ja millaisia velvoitteita edustajalla on suhteessa tietosuojaviranomaisiin, rekisteröityihin ja tuomioistuimiin. Edustajan määritelmää tulisi selventää, jotta pystyttäisiin tarkemmin määrittelemään edustajan toimenkuva ja vastuut.[195]

Tietosuojatyöryhmä kiinnittää 25 artiklan osalta huomiota myös artiklassa määriteltyihin poikkeusperusteisiin, jotka vapauttavat rekisterinpitäjän velvollisuudesta asettaa edustaja. Ongelmallisena tältä osin pidetään ensinnäkin 2a-kohtaa, jossa säädetään, että edustajan asettamisvelvoitetta ei ole sellaisella rekisterinpitäjällä, joka on sijoittautunut sellaiseen maahan, jonka tietosuojan tasoa komissio pitää riittävänä. Tietosuojatyöryhmä ei pidä valittua näkökantaa perusteltuna sillä sen mielestä se, että rekisterinpitäjän sijoittautumismaan tietosuojan taso katsotaan riittäväksi, ei poista tarpeellisuutta unionin alueella olevalle yhteyspisteelle. Se ehdottaakin, että 2a-kohta tulisi poistaa kokonaan.[196]

Myöskään yrityksen koon perusteella tapahtuvaa rajausta[197] tietosuojatyöryhmä ei näe oikeana ratkaisuna. Artiklan 25 2b-kohdan osalta ongelmallisena nähdään tilanteet, joissa alle 250 työntekijän yritykset rajautuisivat edustajan asettamisvelvoitteen ulkopuolelle siitä huolimatta vaikka ne käsittelisivät luonteeltaan ns. korkean riskin henkilötietoja. Samaten 25 artiklan 2d-kohta nähdään liian epämääräisesti määriteltynä ja riskinä olisi, että se saattaisi olla altis väärille tulkinnoille: *rekisterinpitäjään, joka tarjoaa tavaroita tai palveluja unionin alueella asuville rekisteröidyille vain satunnaisesti*. Ratkaisuna edustajan asettamisvelvollisuudesta vapauttamisesta päättämiseen tietosuojatyöryhmä ehdottaa, että huomiota kiinnitettäisiin siihen millaista

[194] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 12-13
[195] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 15
[196] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 15
[197] 25 artiklan 2b-kohta

henkilötietojen käsittely on luonteeltaan ja minkä laajuista toiminta on. Myös se, kuinka isoa rekisteröityjen määrää henkilötietojen käsittely koskee, tulisi päätöstä tehdessä ottaa huomioon. Näillä valintakriteereillä päästäisiin tietosuojatyöryhmän mielestä parempaan lopputulokseen kuin tämän hetkisillä asetusehdotuksen 25 artiklan 2-kohdan rajauksilla.[198]

Tietosuojatyöryhmä ottaa lausunnossaan kantaa myös vastuukysymyksiin. Tietosuojatyöryhmä pitää *erittäin myönteisenä* sitä, että asetusehdotukseen on otettu vastuuperiaate erityisesti 22 artiklan mukaisesti. Sen sijaan niiden artiklojen osalta, joissa vastuuperiaatetta pyritään täsmentämään, löytää tietosuojatyöryhmä huomautettavaa. Seuraavassa olen ottanut käsittelyyn muutaman näistä asetusehdotuksen vastuuperiaatetta täsmentävistä kohdista, joihin esitetään muutoksia.[199]

Asetusehdotuksen 28 artikla käsittelee rekisterinpitäjän velvollisuutta säilyttää henkilötietojen käsittelyään koskevat asiakirjat. Tietosuojatyöryhmä painottaa lausunnossaan, että velvollisuuden säilyttää henkilötietoja käsittelyä koskevat asiakirjat tulisi koskea kaikkia rekisterinpitäjiä, henkilötietojen käsittelijöitä ja mahdollisia rekisterinpitäjien edustajia. Tällä huomautuksellaan tietosuojatyöryhmä viittaa erityisesti 28 artiklan 4b-kohtaan, jossa alle 250 työntekijän rekisterinpitäjät ja henkilötietojen käsittelijät on vapautettu asiakirjojen säilyttämisvelvoitteesta mikäli ne käsittelevät henkilötietoja vain pääasiallisen toimintansa aputoimena. Ongelmana nähdään sama riski kuin jo aiemmin käsitellyssä 25 artiklassa[200] eli riski siitä, että pieni organisaatio, joka käsittelee riskialttiita henkilötietoja jää myös tämän keskeisen rekisteröityä suojaavan järjestelyn ulkopuolelle. Tietosuojatyöryhmä esittääkin myös tässä yhteydessä, että organisaation työntekijämäärän sijasta rajausta tehdessä tulisi huomiota kiinnittää siihen, millaisia henkilötietoja käsitellään ja kuinka laajaa käsittely on.[201]

Toinen vastuukysymyksiä sivuava artikla, jonka tietosuojatyöryhmä on lausunnossaan halunnut nostaa esille, on 33 artikla, joka käsittelee rekisterinpitäjän velvollisuutta määrätyissä tilanteissa tehdä tietosuojaa koskeva

[198] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 15
[199] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 16
[200] Edustajan asettamisvelvoite
[201] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 16

vaikutusarviointi. Tietosuojatyöryhmä katsoo, että 33 artiklan tavoitetta voidaan pitää positiivisena lähtökohtana, mutta tästä huolimatta artiklasta löytyy lukuisia kohtia, joita sen mielestä tulisi muuttaa toimivampaan muotoon.[202]

Ensinnäkin tietosuojatyöryhmä esittää, että 33 artiklan ensimmäinen kohta tulisi muuttaa sanamuodoltaan sellaiseen muotoon, että myös tilanteissa, joissa ei ole täysin varmaa, että henkilötietojen käsittelyyn liittyy rekisteröidyn kannalta erityisiä riskejä, tulisi suorittaa tietosuojaa koskeva vaikutusarviointi. Toiseksi artiklaan tulisi lisätä määräys, että kaikkia asetusehdotuksen 9. artiklassa ns. erityisen arkaluonteisia tietoja käsitellessä, tulisi suorittaa vaikutusarviointi. Tätä edellyttäisi käsiteltävien tietojen erityinen arkaluonteisuus. Kolmantena seikkana 33 artiklan osalta tietosuojatyöryhmä nostaa esille 2-kohdan b, c ja d-kohdissa käytetyn ”suuressa mittakaavassa” määritelmän. Tietosuojatyöryhmän mielestä rajaus, jolla määrätynlaisten tietojen osalta vain ”suuressa mittakaavassa” suoritetut tietojenkäsittelyt on katsottu vaikutusarvioinnin tekemisvelvoitteen alaisiksi, ei ole perusteltu ja se tulisi poistaa kokonaan. Tietosuojatyöryhmä katsoo täten, että kaikissa 33 artiklan toisen kohdan alakohdissa tulisi suorittaa tietosuojaa koskeva vaikutusarviointi toiminnan laajuudesta riippumatta.[203]

Rekisterinpitäjän kannalta asiaa erityisesti tarkasteltaessa on syytä mainita myös tietosuojatyöryhmän lausunnossaan esille nostamat asetusehdotuksen tietoturvaloukkausten ilmoitusvelvollisuutta koskevat 31 ja 32 artiklat. Tietosuojatyöryhmä pitää myönteisenä, että asetusehdotukseen on sisällytetty velvoitteet ilmoittaa tietoturvaloukkauksista sekä valvontaviranomaiselle että rekisteröidylle itselleen. Lausunnossa nostetaan esille kuitenkin huoli siitä, onko näitä velvoitteita koskeva säätely jätetty kuitenkin liian avoimeksi ja tulkinnanvaraiseksi. Tietoturvaloukkauksen luonne ja kriteerit siitä, milloin tietoturvaloukkauksesta tulee ilmoittaa viranomaiselle ja rekisteröidylle olisi määriteltävä tietosuojatyöryhmän mielestä asetusehdotuksessa tarkemmin.[204]

Tietosuojatyöryhmä katsoo, että erityisesti valvontaviranomaiselle tehtävän ilmoitusvelvollisuuden tulisi olla ehdotettua suppeampi, sillä riskinä on, että valvontaviranomaiset ylikuormittuvat erityisesti sellaisista valvontailmoituksista, jotka koskevat sellaisia vähäisiä tietoturvaloukkauksia, jotka eivät

[202] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 16-17
[203] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 16-17
[204] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 17

todellisuudessa vaaranna rekisteröidyn oikeuksia. Lausunnossa kiinnitetään huomiota myös asetusehdotuksen 31 artiklassa määrättyyn 24 tunnin sisällä valvontaviranomaiselle tehtävään tietoturvaloukkausta koskevaan ilmoitukseen. Tietosuojatyöryhmä painottaa sen tärkeyttä, että ilmoitus tietoturvaloukkauksesta toimitetaan nopeasti viranomaisen tietoon. Se kuitenkin myönnetään, että määrätyissä tilanteissa ilmoituksen tekeminen tiukan 24 tunnin määräajan sisällä ei aina välttämättä ole mahdollista. Tähän ongelmaan tietosuojatyöryhmä ehdottaakin ratkaisuksi sitä, että ilmoitus määrättäisiin aina annettavaksi 24 tunnin sisällä, mutta sillä poikkeuksella, että jos kaikkia tietoturvaloukkausta koskevia tietoja ei voida vielä tämän ilmoituksen yhteydessä toimittaa, on ilmoitusta voitava täydentää myöhemmässä vaiheessa.[205]

11 EUROOPAN PARLAMENTIN LAINSÄÄDÄNTÖPÄÄTÖSLAUSELMA

Euroopan parlamentti äänesti 12.3.2014 kannastaan uudeksi yleiseksi tietosuoja-asetukseksi.[206]

Parlamentin hyväksymä päätöslauselma[207] eroaa monelta kohdin siitä mitä komissio on omassa ehdotuksessaan uudeksi tietosuoja-asetukseksi alunperin ehdottanut. Seuraavassa otan tarkempaan käsittelyyn merkittävimmät näistä muutosehdotuksista – erityisesti rekisterinpitäjän kannalta asiaa katsottuna.

Tietoturvaloukkauksien ilmoittamista valvontaviranomaisille koskevaa 31 artiklaa parlamentti ehdottaa muutettavaksi siten, että tarkka 24 tunnin aikaraja jätettäisiin kokonaan pois. Parlamentti katsoo, että aikamääritteeksi riittäisi sanamuotoa ”ilman aiheetonta viivytystä”. Artiklassa Euroopan tietosuojaneuvostolle annettaisiin oikeus määritellä tarkemmat suuntaviivat sille, miten määritelmää ”ilman aiheetonta viivytystä” tulisi käytännössä tulkita. Lisäksi 31 artiklan kolmatta kohtaa, joka koskee annettavan ilmoituksen

[205] Tietosuojatyöryhmän lausunto 1/2012 tietosuojauudistusta koskevista ehdotuksista, s. 17

[206] Euroopan parlamentin lehdistötiedote. Mepit äänestivät vahvemman henkilötietojen suojan puolesta.

[207] Euroopan parlamentti: Euroopan parlamentin lainsäädäntöpäätöslauselma 12. maaliskuuta 2014 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Tavallinen lainsäätämisjärjestys: ensimmäinen käsittely)

sisältöä, ehdotetaan tarkennettavaksi siten, että tietoja ei tarvitsisi antaa kerralla, vaan ne voitaisiin antaa myös tarvittaessa vaiheittain. Valvontaviranomaisen osalta parlamentti edellyttäisi vielä lisäksi, että ilmoitetuista rikkomustyypeistä tulisi pitää julkista rekisteriä.[208]

Parlamentti esittää myös kokonaan uutta artiklaa tietosuoja-asetusehdotukseen. Uusi 32 a artikla käsittelisi erityisen riskialttiiden tilanteiden huomioonottamista. Uuden artiklan voidaan katsoa käsittelevän ainakin osittain artiklaa 33, joka koskee tietosuojaa koskevaa vaikutusarviointia. Parlamentti onkin hyväksymässään muutosehdotuksessa osittain sitonut toisistaan riippuvaisiksi 33 artiklan ja ehdottamansa uuden 32 a artiklan toteutuksen.

Ehdotetun uuden artiklan ensimmäisessä kohdassa määritellään rekisterinpitäjiä – *tarvittaessa* myös henkilötietojen käsittelijöitä – koskeva uusi velvollisuus:

1. Rekisterinpitäjän tai tarvittaessa henkilötietojen käsittelijän on laadittava riskianalyysi suunnitellun tietojenkäsittelyn mahdollisista vaikutuksista rekisteröityjen oikeuksiin ja vapauksiin ja arvioitava, aiheutuuko sen käsittelytoimista erityisiä riskejä.

Artiklan toisessa kohdassa luetellaan yhdeksän eri tapausta joihin katsotaan liittyvän *erityisiä riskejä*. Tällaisina henkilötietojen suojan kannalta erityisen riskialttiina tilanteina mainitaan esimerkiksi sellaiset henkilötietojen käsittelytoimet, joissa käsitellään yli 5000 rekisteröidyn tietoja 12 kuukauden ajanjaksolla sekä toimet, joissa harjoitetaan suuressa mittakaavassa valvontaa joka kohdistuu julkisiin alueisiin.

Laaditun riskianalyysin tuloksesta riippuen rekisterinpitäjä velvoitettaisiin määrätyissä tilanteissa toteuttamaan jatkotoimia henkilötietojen suojaamisen varmistamiseksi. Tällaisina jatkotoimina ehdotetaan artiklan kolmannessa kohdassa rekisterinpitäjän laajennettua velvollisuutta kuulla asiassa tietosuojavastaavaa tai valvontaviranomaista.[209] Lisäksi riskianalyysi tulisi tarkistaa viimeistään vuoden päästä sen laatimisesta *tai välittömästi, jos tietojenkäsittelytoimien luonne, laajuus tai tarkoitus muuttuu merkittävästi*.[210]

Tietosuojavastaavaa koskevia artikloita 35, 36 ja 37 ehdotetaan päätöslauselmassa muutamilta kohdin muutettaviksi. Kysymys on lähinnä

[208] Lainsäädäntöpäätöslauselman tarkistus nro. 125
[209] 34 artiklan mukaisesti
[210] Lainsäädäntöpäätöslauselman tarkistus nro. 127

tarkennuksista, joita parlamentti haluaa tuoda tietosuojavastaavan nimittämistä, asemaa ja tehtäviä koskeviin artikloihin.

Artiklan 35 osalta parlamentti esittää, että komission määrittämä 1b-kohta, jossa tietosuojavastaavan nimittämisvelvoite on sidottu 250 työntekijän vähimmäismäärään, poistettaisiin kokonaan. 1b-kohdan tilalle parlamentti esittää määritelmää, jossa huomioon otettaisiin se kuinka montaa henkilöä oikeushenkilön suorittamat henkilötietojen käsittelytoimet koskevat 12 kuukauden aikajaksolla tarkasteltuna. Tällöin, jos käsittelytoimet koskisivat yli 5000 henkilöä, olisi rekisterinpitäjän nimitettävä tietosuojavastaava. Edellisen lisäksi parlamentti laajentaisi edelleen sitä rekisterinpitäjien ja henkilötietojen käsittelijöiden ryhmää, jonka tulee nimittää tietosuojavastaava, kokonaan yhdellä uudella ryhmällä. Tällainen uusi ryhmä, jolla olisi velvollisuus nimittää tietosuojavastaava, olisi sellaiset rekisterinpitäjät ja henkilötietojen käsittelijät joiden tehtävät koostuvat pääasiassa käsittelytoimista joissa käsitellään ns. erityisiin tietoryhmiin kuuluvia tietoja,[211] sijaintitietoja taikka työntekijöitä tai lapsia koskevia tietoja. Lisäedellytyksenä olisi, että tietojenkäsittely kyseisissä tapauksissa tapahtuisi *suuren mittakaavan rekisteröintijärjestelmissä*.[212]

Edellä mainittujen tietosuojavastaavan nimittämistä selventävien ja laajentavien muutosten lisäksi parlamentti esittää päätöslauselmassaan muutosta minimiaikaan, joksi ajaksi tietosuojavastaava vähintään on nimitettävä. Komission ehdottamaa kahden vuoden minimiaikaa parlamentti soveltaisi pelkästään niihin tietosuojavastaaviin, jotka on rekrytoitu tehtävään organisaation ulkopuolelta eli ts. kysymyksessä olisi tällöin ulkoinen palveluntuottaja, joka tarjoaa tietosuojavastaavan organisaatiolle. Sen sijaan, jos tietosuojavastaavaksi on nimitetty henkilö, joka on rekisterinpitäjän tai tietojenkäsittelijän organisaation työntekijä, olisi parlamentin mukaan tällöin minimiajaksi määritettävä neljä vuotta.[213]

Tietosuojavastaavan asemaa määrittelevää artiklaan 36 esitetään päätöslauselmassa myös muutamilta kohdin muutettavaksi. Ensinnäkin parlamentti katsoo, että artiklan toisen kohdan määritelmä, jossa tietosuojavastaava velvoitetaan raportoimaan toiminnastaan ja havainnoistaan

[211] Tiedot määritelty 9. artiklan ensimmäisessä kohdassa
[212] Lainsäädäntöpäätöslauselman tarkistus nro. 132
[213] Lainsäädäntöpäätöslauselman tarkistus nro. 132

rekisterinpitäjän tai henkilötietojen käsittelijän *johdolle*, ei ole tarpeeksi yksilöivä määritelmä. Parlamentti muuttaisi sanamuodoksi *toimeenpaneva johtoelin*. Lisäksi parlamentti esittää, että rekisterinpitäjä ja henkilötietojen käsittelijä velvoitettaisiin nimittämään organisaation toimeenpanevaan johtoelimeen erityisen jäsenen, jonka erityisenä vastuualueena olisi tietosuoja-asetuksen säännösten toteuttaminen. Artiklan kolmanteen, tietosuojavastaavan resursseja määrittelevään kohtaan, päätöslauselmassa halutaan lisätä sanat *kaikki välineet*. Tällä haluttaneen painottaa vaatimusta siitä, että tietosuojavastaavalle on järjestettävä nimenomaan kaikki hänen tuloksellisen toimintansa edellyttämät resurssit niiden luonteesta riippumatta.[214]

Tietosuojavastaan asemaa koskevaan 36 artiklaan esitetään päätöslauselmassa myös kokonaan uutta alakohtaa, mikä määrittelisi tietosuojavastaavan salassapitovelvollisuuden. Tämän mukaisesti tietosuojavastaavat olisivat salassapitovelvollisia sekä rekisteröityjen *henkilöllisyydestä* kuin myös niistä tilanteista, joista rekisteröidyt ovat tunnistettavissa. Salassapitovelvoitteesta olisi mahdollista vapautua, jos rekisteröity on antanut siihen luvan.[215]

Tietosuojavastaavan pääasiallinen tehtäväsisältö määritellään asetusehdotuksen 37. artiklassa. Parlamentti esittää laajempaa tietosuojavastaavan tehtäväkenttää verrattuna komission esitykseen. Ensinnäkin artiklan 1a-kohtaan, joka koskee tietosuojavastaavan yleistä velvollisuutta antaa neuvontaa rekisterinpitäjälle tai henkilötietojen käsittelijälle koskien tämän asetuksen mukaisia velvoitteita, esitetään lisättäväksi sanat *lisätä tietoisuutta*. Tällä lisäyksellä voitaneen parlamentin katsoa tavoitelleen ajatusta siitä, että tietosuojavastaavan tulee oma-aloitteisesti organisaation sisällä lisätä tietoisuutta tietosuoja-asetuksen velvoitteista – nimenomaan ilman, että rekisterinpitäjän tai tietojenkäsittelijän tulisi määrättyä seikkaa tiedustella. Artiklan 1a-kohtaan on lisätty myös toinen lisäys; *erityisesti teknisiin ja organisatorisiin toimenpiteisiin ja menettelyihin liittyviä* jne. Tällä lisäyksellä päätöslauselmassa on selvästi haluttu painottaa sitä, mitä asetuksen seikkoja erityisesti tietosuojavastaavan tulisi antamassaan neuvonnassa tuoda esille.

[214] Lainsäädäntöpäätöslauselman tarkistus nro. 133
[215] Lainsäädäntöpäätöslauselman tarkistus nro. 133

Vaikka erot komission esittämään sanamuotoon eivät ole merkittäviä on painotuserot tavoitteissa kuitenkin havaittavissa.[216]

Päätöslauselmassa esitetään tietosuojavastaavan vastuulle myös aivan kokonaan uusia tehtäviä. Parlamentti esittää artiklaan 37 kahta uutta tehtävänkuvaa. Ensimmäinen näistä uusista velvoitteista olisi tietosuojavastaavan velvollisuus huolehtia siitä, että tätä asetusta toteutettaessa noudatetaan artiklan 34 mukaista ennakkokuulemisvelvoitetta. Lisäksi toinen kokonaan uusi tehtävä, jota esitetään tietosuojavastaavalle kuuluvaksi, olisi velvollisuus *tiedottaa työntekijöiden edustajille* tietojenkäsittelystä, joka koskee työntekijöitä.[217]

Käytännesääntöjä koskevaa 38 artiklaa parlamentti muuttaisi lähinnä siten, että valvontaviranomaisten asemaa vahvistettaisiin verrattuna siihen, mitä komissio omassa esityksessään on esittänyt. Parlamentti esittää ensinnäkin valvontaviranomaisille itsenäistä oikeutta laatia käytännesääntöjä. Toiseksi valvontaviranomaisen oikeus antaa lausunto suunnitelluista käytännesäännöistä tai niiden muuttamisesta muutettaisiin velvollisuus muotoon. Toisin sanoen valvontaviranomainen ei voisi kieltäytyä antamasta lausuntoa käytännesääntöjen luonnoksesta silloin, kun siltä sitä pyydettäisiin.[218]

Sertifiointia koskevaa 39 artiklaa parlamentti tarkentaisi huomattavasti komission ehdottamasta. Parlamentin mukaan sertifioinnin hankkimisen tulisi olla vapaaehtoista ja kohtuuhintaista. Sertifiointimenettelyjen tulisi olla läpinäkyviä ja menettelyllä ei saisi aiheuttaa *kohtuutonta taakkaa* rekisterinpitäjälle. Päätöslauselmassa ei tosin sen tarkemmin valoteta sitä, mitä kohtuuttomalla taakalla tarkoitetaan, mutta sen voitaneen tulkita tarkoittavan ainakin taloudellisia menoeriä, joita sertifioinnin hankkimisesta väistämättä aiheutuu. Sertifioinnin voimassaololle asetettaisiin lisäksi viiden vuoden enimmäisaika, jonka sertifiointi voisi kerrallaan olla voimassa. Lisäksi esitetään, että Euroopan tietosuojaneuvoston olisi perustettava julkinen rekisteri, josta kävisi ilmi kaikki voimassa olevat sertifioinnit. Euroopan tietosuojaneuvostolle annettaisiin myös oikeus määrätyissä tilanteissa myöntää tietosuojasertifikaatteja. Parlamentti sitoisi lisäksi komissiolle ehdotetun

[216] Lainsäädäntöpäätöslauselman tarkistus nro. 134
[217] Lainsäädäntöpäätöslauselman tarkistus nro. 134
[218] Lainsäädäntöpäätöslauselman tarkistus nro. 135

oikeuden säätää tarkempia säädöksiä koskien sertifiointimenettelyjä menettelyyn, jossa pakollisena vaiheena olisi Euroopan tietosuojaneuvostolta lausunnon pyytäminen sekä sidosryhmien ja riippumattomien järjestöjen kuuleminen.[219]

12 LOPUKSI

On selvää, että nykyisin voimassa olevan henkilötietolain sisältö on käynyt auttamatta vanhaksi. Se ei vastaa sisällöltään enää niitä vaatimuksia, joita henkilötietojen suojalta voidaan perustellusti nykypäivänä vaatia. Syynä tähän voidaan erityisesti pitää viime vuosikymmenen aikana tapahtunutta voimakasta teknologian kehitystä. Kun henkilötietolakia säädettiin 90-luvun loppupuolella moniakaan tämän päivän teknologisia innovaatioita ei ollut vielä olemassa. On selvästi nähtävissä, että henkilötietolaissa ei osattu vielä varautua kaikkiin niihin ongelmatilanteisiin, joita teknologian nopea kehitys on yksityisyydelle aiheuttanut.

Siitä, millä tavoin nykyisin voimassa olevaa henkilötietojen suojaa koskevaa lainsäädäntöä tulisi unionitasolla uudistaa, ollaan montaa mieltä. Tämän osoittaa varsin selvästi jo tässä tutkielmassa käsittelyyn otetut virallisraportit, joissa esitetään lukuisia – myös toisistaan huomattavasti eroavia – muutosehdotuksia alkuperäiseen asetusehdotukseen. Yhdistävänä tekijänä näille raporteille on kuitenkin yhteinen mielipide siitä, että nykyistä lainsäädäntöä tulee uudistaa. Myös se, että uudistusten tulee olla suuruusluokaltaan huomattavia, on yhteistä kaikille näille käsitellyille kannanotoille. Eroavaisuudet tulevat esille siinä millaisia uudistusten tulisi olla sisällöltään.

Kun on kysymys uudistusten toteuttamisesta, voitaneen perustellusti esittää kysymys; mistä mielipide-eroavaisuudet sitten johtuvat? Mielestäni keskeisenä seikkana voidaan pitää eturyhmien toisistaan poikkeavia intressejä. Asetusehdotusta käsitteleviä kannanottoja on laadittu lukuisten eri tahojen toimesta. Tutkielmassani olen ottanut näistä vertailuun vain muutaman keskeisen. Eri kannanotoissa painottuu eri seikat, sen mukaan millaisia eturyhmiä kussakin kokoonpanossa on ollut edustettuina. Vaikka kannanottoja

[219] Lainsäädäntöpäätöslauselman tarkistus nro. 136

laadittaessa pyrittäisiinkin neutraaliin näkökulmaan, on kuitenkin luonnollista, että poliittiset näkökannat antavat oman vivahteensa kannanotoille.

Rekisterinpitäjiä edustavien tahojen kannalta uudistusta tarkasteltaessa on varsin selvää, että tällöin painottuvat näkökannat, joissa painotetaan rekisterinpitäjien velvoitteiden mahdollisimman kevyttä ja joustavaa rakennetta. Jos rekisterinpitäjien velvoitteita lisätään merkittävästi, on selvää, että velvoitteista aiheutuu samassa suhteessa myös lisäkustannuksia rekisterinpitäjille. Merkittävältä kustannusten lisääntymiseltä halutaan luonnollisesti välttyä. Kannanotoissa ei välttämättä kuitenkaan tuoda suoraan julki lisäkustannusten pelkoa, mutta rivien välistä se on määrätyissä tilanteissa luettavissa.

Tietosuojauudistuksen keskeisimmiksi tavoitteiksi on asetettu tietosuojaa koskevan sääntelyn yksinkertaistaminen ja yhdenmukaistaminen sekä rekisterinpitäjiä velvoittavan byrokratian vähentäminen. Rekisterinpitäjät ovat tietosuojauudistuksen valmisteluvaiheessa tuoneet kuitenkin julki pelkonsa siitä, että uusi asetus saattaa lisäämällä sääntelyä luoda entistä byrokraattisemman toimintaympäristön. Tästä esimerkkinä esiin on nostettu ns. tilivelvollisuuden periaate, jossa rekisterinpitäjän on itse kyettävä jälkikäteen osoittamaan, että kaikissa henkilötietojen käsittelyn vaiheissa on noudatettu lakia. Toisena rekisterinpitäjän taakkaa kohtuuttomasti lisäävänä uudistuksena on nähty korkeat sanktiomaksut, jotka voidaan määrätä rekisterinpitäjälle tilanteessa jossa on rikottu lakia. Sanktiomaksujen osalta on niiden mahdollisen kohtuuttomuuden lisäksi erityisesti huomiota kiinnitetty siihen, että Suomessa perinteisesti lähtökohtana vahingonkorvauksissa on ollut aiheutetun vahingon suuruus, kun taas asetusehdotuksessa lähtökohdaksi on selvästi asetettu niiden sanktiomainen luonne.[220]

Toisaalta kun henkilötietojen suojaa koskevaa uudistushanketta katsotaan rekisteröidyn näkökulmasta uudistuksessa painottuvat varsin erilaiset näkökannat. Tällöin keskeiseksi nousee yksityisyyden suojaamiseen liittyvät lähtökohdat niin tehokkaassa muodossaan kuin vain mahdollista – rekisterinpitäjille aiheutuvista kustannuksista juurikaan välittämättä. Tällöin keskeiseksi nostetaan näkökulmat, joissa painotetaan rekisterinpitäjän ”ankaraa

[220] Männikkö (2012), s. 28-30

vastuuta” henkilötietoja käsiteltäessä. Näissä näkökulmissa uudistetut säännökset pyritään saattamaan sellaisiin muotoihin, jotka turvaavat rekisteröidyn aseman mahdollisimman tehokkaasti. Tällaisista tavoitteista esimerkkinä voidaan mainita varsin laaja rekisterinpitäjää koskeva korvausvelvollisuus sekä tarkat aikarajat omaava tietoturvaloukkauksia koskeva ilmoitusvelvollisuus.

Euroopan parlamentin täysistunnon päätöslauselman hyväksyminen merkitsi käytännössä sitä, että tietosuojaa koskeva uudistushanke etenee toukokuun Euroopan parlamentti vaalien tuloksesta riippumatta vaikka parlamentin poliittiset voimasuhteet muuttuisivat. Parlamentin päätöslauselman hyväksymisen tuomasta huomattavasta edistyksestä huolimatta on tietosuojauudistuksen vahvistaminen vielä kesken. Tullakseen voimaan Euroopan neuvoston tulee äänestää yhteispäätösmenettelyn mukaisesti tietosuoja-asetuksesta ja direktiivistä.[221]

Kuinka ison muutoksen uudistushanke loppujen lopuksi tuo tietosuojalainsäädäntöön? On selvää, että vastaus riippuu siitä, minkä unionin maan tietosuojalainsäädännön kannalta asiaa tarkastelee. Suomessa tuleva tietosuoja-asetus ei Reijo Aarnion mielestä tuo ainakaan näillä näkymin kovin valtavaa muutosta nykytilanteeseen. Hän muistuttaakin, että moni uudistuksessa mukana oleva seikka on huomioitu jo nykyisellään henkilötietolaissa.[222]

Henkilötietojen suojaa koskevaa uudistushanketta eteenpäin vietäessä olisi syytä pitää mielessä, että keskeisenä lähtökohtana uudistushankkeelle on ollut – ja tulisi edelleen olla – yksilön suojaaminen. Yksilön yksityisyyden suoja ja muut oikeudet tulisi varmistaa riittävän tehokkaalla tavalla. Ei ole hyväksyttävää, että taloudellisiin seikkoihin vetoamalla merkittävästi joustettaisiin siitä korkeasta henkilötietojen suojan tasosta, jota uudistuksella tavoitellaan. On toki myönnettävä, että lainsäädäntöhankkeisiin liittyy aina useita eri intressiryhmiä ja näkökantoja. Unionin tasolla toteutettava henkilötietojen suojaa koskevan lainsäädännön uudistushanke ei ole tästä poikkeus. On selvää, että uudistushanketta loppuun saatettaessa myönnytyksiä on tehty puolin ja toisin.

[221] Euroopan unionin komission lehdistötiedote. Progress on EU data protection reform now irreversible following European Parliament vote.
[222] Männikkö (2012), s. 37

Päättäjien on kuitenkin pystyttävä – merkittävistäkin eturistiriidoista huolimatta – saattamaan voimaan säädöskokonaisuus, jossa yksilön oikeudet henkilötietojen käsittelyssä on turvattu tämän päivän tietoyhteiskunnan vaatimien korkeiden standardien mukaisesti.